NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A SIMULATION ON ORGANIZATIONAL COMMUNICATION PATTERNS DURING A TERRORIST ATTACK

by

Ali Bas
Volkan Karaca

June 2008

Thesis Advisor:	Deborah E. Gibbons
Co-Advisor:	James E. Suchan

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE A Simulation on Organizational Communication Patterns During A Terrorist Attack			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ali Bas, Volkan Karaca			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The purpose of this project is to provide a simulation which includes communication structures during a terrorist attack. Different communication patterns will provide different results in terms of effectiveness and efficiency. We are planning to identify some key variables to form an effective network structure in a military action. According to key variables of an organization, centralized and decentralized structures produce different communication patterns and different outputs as well. In a combat environment these different patterns will result in distinct results in terms of effectiveness and efficiency. This environment can be modeled by the help of software like Arena.

As a part of the Global War on Terrorism NATO forces are conducting operations in Afghanistan. To enhance stability in Afghanistan, NATO established PRTs (Provincial Reconstruction Teams) composed of multinational elements (partly civilian, but mostly military. These teams are static, and form potential targets for terrorist attacks. We will use PRTs in our model as the target of the terrorists and try to discriminate communication structures in these ambush scenarios.

14. SUBJECT TERMS Network, centralized, decentralized, PRT, Afghanistan, NATO, terrorism			**15. NUMBER OF PAGES** 79
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A SIMULATION ON ORGANIZATIONAL COMMUNICATION PATTERNS DURING A TERRORIST ATTACK

Ali Bas
First Lieutenant, Turkish Air Force
Industrial Engineering, Turkish Air Force Academy, 2001

Volkan Karaca
First Lieutenant, Turkish Air Force
Electronic Engineering, Turkish Air Force Academy, 2002

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Authors:

Ali Bas

Volkan Karaca

Approved by:

Deborah E. Gibbons
Thesis Advisor

James E. Suchan
Co-Advisor

Robert N. Beck
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this project is to provide a simulation which includes communication structures during a terrorist attack. Different communication patterns will provide different results in terms of effectiveness and efficiency. We are planning to identify key variables to form an effective network structure in a military action. According to key variables of an organization, centralized and decentralized structures produce different communication patterns and different outputs as well. In a combat environment these different patterns will result in distinct results in terms of effectiveness and efficiency. This environment can be modeled with the help of software like Arena software.

As a part of the Global War on Terrorism NATO forces are conducting operations in Afghanistan. To enhance stability in Afghanistan, NATO established PRTs (Provincial Reconstruction Teams) composed of multinational elements (partly civilian, but mostly military). These teams are static, and form potential targets for terrorist attacks. We will use PRTs in our model as the target of the terrorists and try to discriminate communication structures in these ambush scenarios.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express our highest appreciation to Professor Deborah E. Gibbons, our thesis advisor, for her invaluable guidance, excellent support and availability at all times throughout our project study. This work could never be completed without her contributions, comments and reviews.

We would also like to thank Professor James E. Suchan, as the associate advisor for our project and his valuable comments and contributions.

Lt. Ali Bas:

First I would like to thank my lovely wife Kubra for sustaining me with her patience and support with her constant love. And I would like to thank my parents for their continued support of my career and interests, particularly for their support of the time associated with this project. Also I would like to thank my thesis partner Volkan for his hard work and dedication throughout this project. My heartfelt thanks go to my beloved ones and my friends for their continuous belief and moral support.

Lt. Volkan Karaca:

This has been one of the most wonderful and enriching experiences of my life. I would like to thank my wife, Tugba, for her dedicated support over the duration of my entire education and research at NPS. Her encouragement and understanding was invaluable. I also want to thank my thesis partner, Ali, who initiated this project and developed the project with his ideas.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

At the end of the 20th century, the industrial age gave way to the information age. This new information age has caused new approaches to many aspects of our economic, social, legal, and political lives. One of the most important characteristics of this age is information exchange. This focus on information exchange raises an interesting dynamic which will affect all aspects of our lives: networks.

Although networks affect nearly all facets of our lives, our concern is military networks. In the modern world, all military activities are controlled by the help of networks. This approach introduces an important concept named Network Centric Warfare (NCW). Network Centric Warfare has become a reason for military strength in the last decades. This concept includes a set of notions which are abbreviated as C4ISR (command, control, **communication,** computer intelligence, and surveillance reconnaissance). This concept first started with C2 and become C3, C4 and eventually C4ISR in a short period of time. Our focus within that concept is, generally, communication.

Basically, a communication network is formed by nodes and the connections between them. There is information flow through some units. As relates to its communication aspects, NCW can be classified according to two different variables of military organization. One of them is homogenous and heterogeneous characteristics of the organization. The other one is value-symmetric and non-value symmetric units in the military force unit. NCW architecture is value-symmetric if all nodes have the same value, in the sense that the loss of any one node is as serious as the loss of any other. NCW architecture is non-value-symmetric if some nodes are more critical than others. NCW architecture is homogenous if all the nodes are identical and heterogeneous if all the nodes are different. Simply put, identical nodes have same specialties, capabilities, and professions (Dekker, 2005).

In order to improve the capabilities of a network we need to assess the effects of various kinds of network patterns on outcomes of interest. This task would be nearly impossible in a combat setting, and the delay required to gather enough data for rational decision making would be unacceptable. Instead, we created simulations based on the scenarios from an example where the terrorist attacks are the biggest challenge and the military networks are very important. In these scenarios we examined various kinds of network structures under the circumstances of terrorist actions in a virtual environment that is identical with a real world example. Our goal in this project is to provide a unique analysis of military network configurations in terms of efficiency and effectiveness.

B. MOTIVATION

One of the most important military alliances in the world, with its multinational perspective, is NATO. After 9/11 the global threat was transformed, and NATO needs to transform as well. This huge organization is experiencing many problems and challenges in Afghanistan, which is an expeditionary operation. NATO's positive transformation could be indicated by success with this new threat, but the desired success has not yet occurred. Afghanistan is one of the most important joint actions in the recent history of NATO.

Burden sharing has been seen as the major problem in Afghanistan for NATO forces by the international organizations. Information exchange is an important part of the burden sharing problem. The military units in Afghanistan have to be part of fully functional military networks in order to overcome the Taliban forces.

Another problem which is important for network centric logistics is the resource and funding problem in Afghanistan. Information exchange and logistics are two interconnected issues that modern military networks must cope with.. Information exchange and resource allocation problems related with networks and the efficiency of networks are the interest of this paper.

We built a pilot scenario situated in Afghanistan to show the potential improvements for organizational network structures in a challenging environment. Combat areas involve uncertainty. Ability to respond quickly and appropriately to uncertainty is crucial for success during combat. To clarify which preparations should be made to improve the probability of successful response to uncertainty, simulation software is a helpful tool.

Information exchange in a multinational organization brings with it the issue of reliability in their connections during an emergency, because of language handicaps, electronic counter measures, etc. That uncertain rate of successful information flow partly creates the various levels of reliability. We will evaluate network performance given different levels of reliability in their communication ties.

Strategy in the combat area is being enabled by the move toward more highly integrated force networks that combine information superiority and advances in technologies for surveillance, communications, precision weapons, and other areas to gain the advantage and rapidly defeat the enemy (Curtin, 2004). The appropriate network structure should enable a feasible strategy and a rapid reaction opportunity to defeat the enemy. We want to show the differences of network patterns in that particular military area with a particular scenario which includes information flow during a combat emergency. The concept of warfare in those scenarios with different network patterns is attempted for a particular area in Afghanistan and modeled using a simulation program application called ARENA®. The resultant output provides insight into network structure effects and the properties of each structure with the effectiveness tool.

C. PROBLEM STATEMENT

This research endeavors to clarify the properties of military network taxonomy with different levels of reliability in a particular case for NATO in Afghanistan. Network taxonomies include fully connected (all channel), centralized (hierarchical), decentralized (selective communication), and random (Dekker, 2005). In the current study, the number and direction of ties, the reliability of ties, and the overall pattern (decentralized versus hierarchical) are varied. Some specific problems which NATO must face provide the changing environment for our experiments and scenarios. As a result of our research, we would like to show the effects of these factors on cost and effectiveness.

Given uncertainty about timing and the extent of potential terrorist attacks, appropriate network design may positively affect NATO's capabilities for response. Likely mechanisms for improving response capability include reaction speed, decision making flexibility, and the control of information flow. Hopefully, as Dodds, Watts, and Sabel (2003) defined network effectiveness, the resultant output provides a recommendation which will maximize effectiveness by minimizing the costly links needed to support a defined burden for our multinational troops in Afghanistan.

D. OBJECTIVES & METHODOLOGY

The analysis intends to achieve the following primary objectives:

1. Characterization of the Problem Space (Input reliability): According to a scenario, different kinds of attacks and different kinds of reactions as well as the network structure will be simulated in this research. The research question in this paper is related to the network structure and its feasibility. But characterization of a real problem space will determine its feasibility. Within this objective, the input gathering phase of this research should correspond with the real combat world.

2. Experiment Design (Strategy): The factors that will give the shape of networks should be involved in the experiments. Technical data from previous work, which will be integrated into this research, will shape the research design. The scenarios of different network patterns should provide interpretable outputs. With the factors of each scenario, a research design will be represented and implemented by the simulation software.

3. Analysis and Recommendation: The interpretation of results will provide valuable recommendations for NATO and also for Turkish and U.S. units in Afghanistan.

The methodology for this project will consist of a comprehensive literature review, simulation model development using ARENA, interpretation of the data generated from the simulation, and recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. AFGHANISTAN AND TERRORISM

A. BACKGROUND OF CONFLICTS IN AFGHANISTAN

The War in Afghanistan is the first and biggest conflict of the 21st century. The current situation began in October, 2001 in response to the September 11, 2001 terrorist attacks on the United States. The main opponent in Afghanistan now is the Taliban (a word meaning “students”), a group formed by a former fighter against the Soviet-backed Afghan Communist regime. Returning to his home village after the defeat of that regime, this member of the Pashtun ethnic group organized his new armed group according to a distorted Islamic view. The Taliban is trying to impose many restrictions on freedom, in line with its strict religious ideology. This group also attracted the support of Osama bin Laden’s al Qaeda organization, thus linking it to 9/11.

By 1997, Pakistan, Saudi Arabia and the United Arab Emirates recognized the Taliban as the legitimate government of Afghanistan. After a dispute with Iran, in 1998, following the terrorist bombings of American embassies in Africa, the United States launched a cruise missile attack on al Qaeda training camps in Afghanistan.

On September 9, 2001, Northern Alliance (the main opposition group to the Taliban) leader Ahmad Shah Massoud was mortally wounded in an assassination attempt performed by two Arab men posing as journalists. This attack was probably the plan of bin Laden's organization. The Northern Alliance responded to Massoud's assassination with an aerial attack on Kabul the night of September 11. It is now known that the assassination of Massoud was planned as a prelude to the terror attacks on the United States which happened on September 11. As the United States assigned blame for the attacks to bin Laden and al Qaeda, plans began to take the fight to al Qaeda and its Taliban sponsors as the first phase of what became known as the Global War on Terror (The War in Afghanistan: Operation Enduring Freedom 2001-Present, 2007).

After the September 11, 2001 attacks on the World Trade Center and the Pentagon, the United States military entered into a war against global terrorism. The

President of the U.S. began the U.S. response with a stroke of his pen, authorizing seizure of the terrorists' financial assets and disruption of their fundraising network (Operation Enduring Freedom – Afghanistan, 2008).

B. NATO AND ISAF IN AFGHANISTAN

The International Security Assistance Force (ISAF) was created at the Bonn Conference, in December 2001, after the overthrow of the Taliban regime. After this conference Afghan opposition leaders' began the process of reconstructing their country by establishing a new government structure, namely the Afghan Transitional Authority. The U.N.-mandated ISAF was launched to provide a safe and secure environment conducive to free and fair elections, the spread of the rule of law, and the reconstruction of the country. The major role of this organization is to maintain and expand security throughout the country, to support stabilization, reconstruction and nation-building activities, and to co-operate with the International Organizations and Non-Governmental Organizations (NGOs) (NATO in Afghanistan Factsheet, 2007).

NATO involvement began in Afghanistan by taking command and coordination of the International Security Assistance Force (ISAF) under U.N. mandate in August 2003. Like its predecessors, it calls upon NATO to disarm militias, reform the justice system, train a national police force and army, provide security for elections, and combat the narcotics industry. Some non-NATO states, such as Australia and New Zealand, contribute resources such as troops to the allied effort. Over time, the alliance has developed four stages, described below, to bring most of Afghanistan under NATO control. NATO leaders have faced considerable difficulty in persuading allies to contribute forces to ISAF, leading to huge resource problems.

In Stage One, 2003-2004, NATO's efforts started in the northern part of the country; French and German forces predominate in these areas. Stage Two began in May 2005, when NATO moved into western Afghanistan; Italian and Spanish forces are the basis of the NATO force there. These sections of the country are relatively stable and have less terrorist incidents than the other areas. Stage Three began in July 2006 when ISAF moved into southern Afghanistan, where U.S., British, Canadian, and Dutch forces predominate. Stage Four began in October 2006, when ISAF took control of the entire country. Meanwhile, the U.S.-led Operation Enduring Freedom (OEF) continues to conduct combat operations in border regions still under threat.

NATO's mission in Afghanistan is seen as a test of the allies' military capabilities and their political will to undertake a complex mission. NATO is seeking to be a "global actor" in its geographic reach and in the development of non-member partner states that assist in achieving an agreed on mission. ISAF represents a test of its ability to be such an actor. By December 2007, ISAF had an estimated 41,700 troops from 39 countries, with NATO members providing the core of the force. The United States has approximately 15,000 troops in ISAF.

NATO's effort in Afghanistan is the alliance's first "expeditionary" mission beyond Europe. The purpose of the mission is the stabilization and reconstruction of Afghanistan. Although NATO has committed stabilization and reconstruction missions previously, for example in Kosovo, the scope of the commitment in Afghanistan is considerably more difficult. The Taliban and remaining al Qaeda continue to resist the operation; Afghanistan has never had a well-functioning central government; and the distance from Europe and the country's geographical difficulties present hard hurdles. For that reason, reconstruction must take place while combat operations continue. And although the allies agree upon a common political objective, some have different interpretations of how best to achieve it. The mission in Afghanistan is important for NATO's future, and for U.S. leadership of the alliance (Gallis, 2008).

After initial military success, since 2005 coalition forces (OEF, ISAF and NATO) have increasingly encountered terrorist attacks by re-emerging Taliban insurgents. In 2006 forces faced their heaviest combat engagements in Afghanistan since the beginning of coalition operations. NATO was forced to conduct intensive ground combat operations in southern Afghanistan, a high risk area (Noetzel, House, & Scheipers, 2007).

At the NATO summit in Riga, Latvia, in November 2006, allied leaders were willing to reduce the caveats that prevent the involvement of outpost in combat in Afghanistan. The United States, Canada, Britain, and the Netherlands have forces in southern and eastern Afghanistan, highly unsettled areas, and have appealed to other governments to release combat forces to assist them in moments of danger. The French government reduced its same caveats and agreed to release its forces in Kabul and elsewhere to come to the assistance of other NATO forces in an emergency. Germany also permits its forces to respond in an emergency. The Italian and Spanish governments said that their force commanders in the field could make the decision to send forces to assist in an emergency situation. It remains unclear whether and when these commanders would have to request approval from their capitals to do so, a confusing factor that could delay a decision (Gallis, 2008).

As the previous information makes clear, Afghanistan presents a growing challenge to NATO. After 2006, Taliban attacks have increased in scope and number, and Taliban fighters are adopting some of the strategies, such as roadside bombs, used by insurgents in Iraq. The Karzai government in Afghanistan is coming under international criticism, and its public support has declined, due to corruption and an inability to improve living conditions. The allies are not in full agreement how to counter these problems, but allied officials say that they need a strong and reliable Afghan government to provide reasonable services and competence to the population if NATO is to succeed (Gallis, 2008).

C. PROVINCIAL RECONSTRUCTION TEAMS

The origin of Provincial Reconstruction Teams is the “Coalition Humanitarian Liaison Cells” that the U.S. military forces in Operation Enduring Freedom established in early 2002. The first Provincial Reconstruction Team (PRT) was settled in Gardez in November 2002 and PRTs in Bamian, Kondoz, Mazar-e-Sharif, Kandahar, and Herat followed in early 2003. The primary purpose of creating these outposts was political, but PRTs were also seen as a means for challenging the causes of Afghanistan’s instability: terrorism, warlords, unemployment, and grinding poverty.

In February 2003, the U.S. Embassy in Kabul published a general set of parameters in a document entitled Principles Guiding PRT Working Relations with United Nations Assistance Mission in Afghanistan (UNAMA), NGOs and Local

Government. These principles established three primary objectives for the PRT program: extend the authority of the Afghan central government, improve security, and promote reconstruction. The PRT Executive Steering Committee, chaired by the Afghan Minister of the Interior, approved these objectives.

The PRTs don't have a central coordinating authority, a governing concept of PRT operations, or a strategic plan. Each sponsoring country has been free to interpret the overall guidelines and to conduct operations based on its national priorities and the local situations. This approach brought beneficial flexibility, but it also resulted in an ad hoc approach to Afghanistan's needs for security and development. This consideration raised the issue of network problems, including the desire to seek improvement in the capabilities of the PRT outposts (Perito, 2005)**.** This paper's objective is to address that requirement.

NATO officials define Provincial Reconstruction Teams (PRTs) as the "leading edge" of the allies' effort to stabilize Afghanistan. Some allied governments believe that lack of effective governance, rather than an insurgency, is the principal problem preventing stabilization of the country. NATO's assistance to the Afghan government in fighting the narcotics trade, disarming militias, reducing corruption, and building an economic infrastructure is the basis of the effort to bring stability to the country. The purpose of the PRTs is to **extend the authority** of the central government into the countryside, provide **security**, and take responsibility for projects (such as **infrastructure development**) to improve the Afghan economy (Gallis, 2008).

Given the importance of establishing a stable environment in Afghanistan, it is surprising that the security role assigned to PRTs was restricted to providing for their own protection. PRTs were not tasked with protecting Afghans, UNAMA or representatives of international relief organizations. They were excluded from conducting eradication and other "enforcement" activities in the counternarcotics effort. They were not expected to track and engage insurgents or other troublemakers.

In addition to their limited mandate, the PRTs' small size restricted the scope of their security-related activities. In the early stages of the program, a single PRT was responsible for a group of neighboring provinces. This meant that PRT units could send only small teams of soldiers on random visits to distant parts of their Provinces of Responsibility. Later, each PRT's area of interest decreased as more were established, but distance, poor roads, mountainous terrain, and harsh winters limited the scope of PRT operations. In spite their restrictive mandate and practical limitations, PRTs played a positive role in providing security and helping to develop the security environment.

The size and composition of U.S. PRTs vary depending on experience, local situations, and the availability of personnel from civilian agencies. According to the model, each U.S. PRT, which has a complement of between 82 and 240[1] American military and civilian personnel, is commanded by an Army Lt. Colonel. There is also an Afghan Ministry of the Interior (MOI) representative and three to four local translators. The model's civilian component includes representatives from the Department of State, the Agency for International Development (USAID), and the Department of Agriculture (USDA) (see Figure 1).

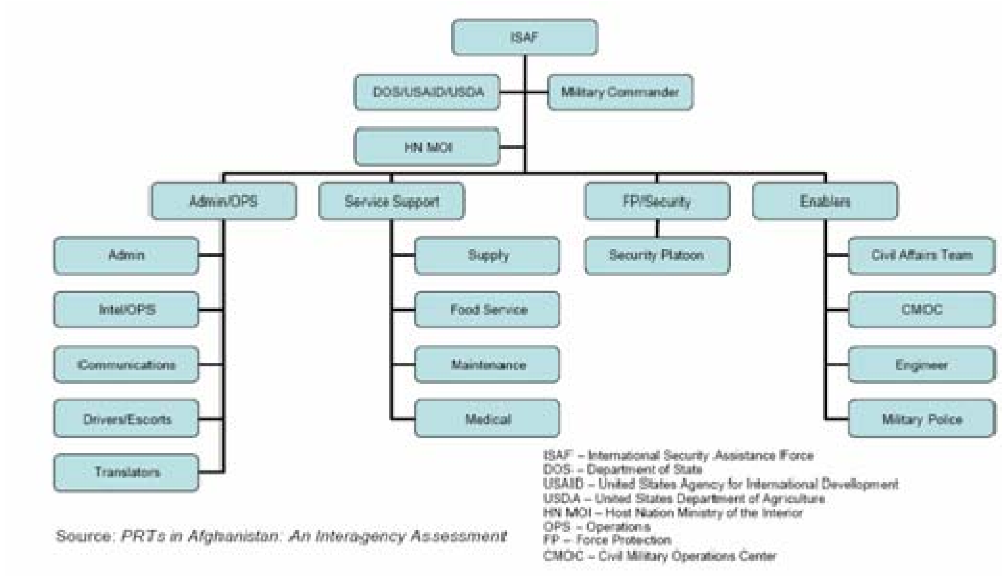


Figure 1. Example PRT organization (From: U.S. Joint Forces Command Joint Warfighting Center, 2007).

[1] According to the Special Report of the U.S Institute of Peace (March 2004) p.4, a PRT can be formed of up to 240 personnel.

The PRT's military component is intended to include the following staff:

- Commanding officer and his immediate staff
- Army Civil Affairs Teams (two teams, four soldiers on each team)
- Military Police Unit (three soldiers)
- Psychological Operations Unit
- Explosive Ordnance/De-mining Unit
- Intelligence Team
- Medics
- Force Protection Unit (infantry platoon of forty soldiers)
- Administrative and support personnel

PRT obligations were subject to the caveat "where expertise and resources permit" and limited to observing and reporting to their superiors, or providing advice and information to Afghan authorities. Lack of skilled personnel was a significant constraint on PRT effectiveness (Perito, 2005).

By most accounts, ISAF PRTs differ significantly from those of the United States. While their mission is the same, their resources and activities are not. Some U.S. officials believe that most European-led PRTs are too hesitant in their engagement of the Afghan population. Some European-led PRTs are minimally funded, or provide little supervision of how their funds are managed and dispensed (Gallis, 2008). For that reason the PRTs are different from each other in the term of capabilities and effectiveness.

PRTs are the most important and network-relevant parts of ISAF They are exchanging information with each other and sending support in their area of responsibility. In terms of resources PRTs are experiencing logistics problems. These problems can be mitigated by more efficient and effective usage of assets, with the help of effective network design. So PRTs in Afghanistan are appropriate candidates for experimental modeling to determine optimal network structures.

The southern part of Afghanistan has the highest risk of terrorist attacks, but we chose to model the area east of Kabul which has a moderate risk of attack. This area includes five U.S. operated and one Turkey operated PRT (see Figure 2). The area is between Kabul and the Pakistan border, and in 2007 10% of incidents occurred in that area. The reason to choose this area is the distance between headquarters and PRTs. The distance will be an important factor in our research design that is described in the following chapter.

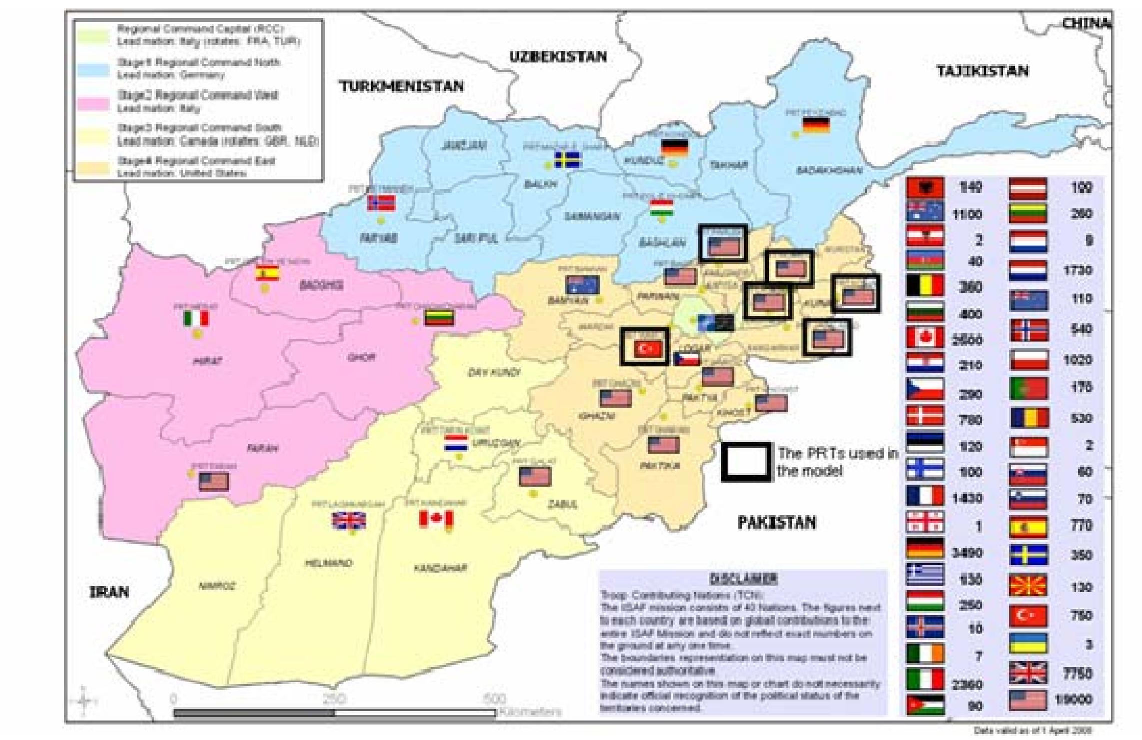


Figure 2. Afghanistan ISAF RC and PRT locations (From: NATO, 2008)

D. MILITARY FORCES AND INFORMATION NETWORKS

Network Centric Warfare (NCW) is defined as follows by the United States Department of Defense:

> Network Centric Warfare (NCW) is an information superiority-enabled concept of operations that describes the way U.S. forces organize and fight in the information age. NCW generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. NCW translates information superiority into combat power by effectively

> linking friendly forces within the battlespace, providing a much improved shared awareness of the situation, and enabling more rapid, effective decision making (U.S. Department of Defense, 2003, p. 2).

Military organizations recognize the need for strategic development of information network structures to support rapid delivery of forces and resources in response to crises (McEnerney, 2001). The overarching goal is to develop flexible systems that deliver necessary assistance without wasting resources or incurring losses because of inefficiency or tardiness. Simulation models that are statistically interpretable but non-trivial and non-obvious can identify appropriate system configurations and provide guidelines for development of assistance networks among humanitarian and military organizations. Our simulations will produce a general model of network effectiveness and efficiency, as well as a specific model for NATO's Provincial Reconstruction Teams (PRTs) in the eastern region of Afghanistan.

E. NETWORK STRUCTURES AND INFORMATION TRANSFER

The structure of a network influences the speed with which crucial information reaches members of the network (Gibbons, 2007a). Two major characteristics that can affect the way a network functions are its density and its centralization. Density is equivalent to the number of ties among players as a percentage of the possible number of ties among them. In general, higher density in a network increases the number of messages that network members receive, but the distribution of these messages is affected by the pattern of the ties.

If the ties are evenly distributed, members generally receive a similar number of messages. Greater variance in number of ties among network members indicates more centralization in the network at large. Specifically, degree centralization measures the extent to which network members vary in their number of ties. Prior research has identified some circumstances under which centralization can be helpful, and some circumstances under which a decentralized network is likely to perform better.

Networks have often been classified according to their level of centralization (Kwon, Oh, & Jeon, 2007; Blau & Scott, 1962) (see Figure 3). For example, random and small-world network structures are decentralized, whereas formal hierarchies and scale free (e.g., Barabasi, & Albert, 1999) networks are centralized. Small world networks are highly clustered, but the minimum distance between any two randomly chosen nodes in this kind of network is shorter when compared to random networks. In scale free networks, the node connections are not homogeneously distributed and , instead, concentrated on certain key nodes. Well-known network prototypes include the All-Channel (fully connected), Circle (connections to adjoining members) and Wheel (hub and spokes, with one central member connecting all others) structures. Both the All-Channel and the Circle structure are decentralized. The Wheel is maximally centralized, as one member has ties to all others, who have no other connections. Within organizations, the All-Channel structure is less stable than the Wheel structure because the more restrictions imposed on communication channels provide for more stable groups (Guetzkow, & Simon, 1955).

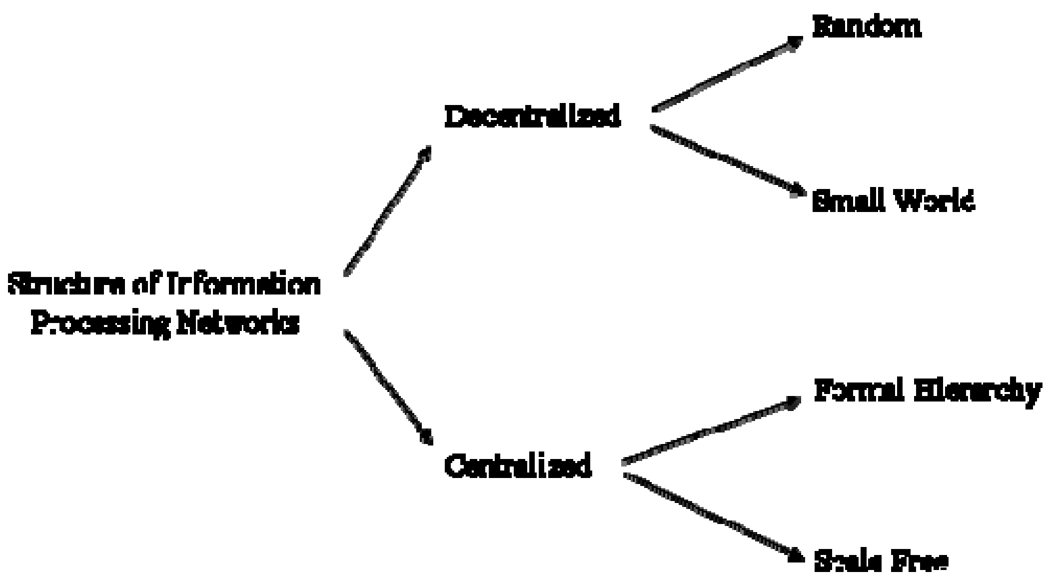


Figure 3. Taxonomy of information processing networks

F. COMPARISON OF CENTRALIZED AND DECENTRALIZED NETWORK STRUCTURES

Information flow can be more economical and more efficient in centralized organizations that consume fewer resources than do decentralized organizations (Arrow, 1974). While decisions are made by coordinators in centralized organizations, specialists often make decisions in decentralized organizations. Because coordinators often have a broad span of control over assets, they are better qualified for some kinds of decision making than are specialists. In these situations, decision making should be processed hierarchically (Hart, & Moore, 2005). Hierarchical network structures can increase efficiency (Bolton, & Dewatripont 1994), possibly because they avoid delays or duplications in information processing that tend to occur in decentralized systems (Bolton, & Farrell, 1990). Further, highly centralized organizations process some tasks, such as finding simple group solutions, faster than decentralized organizations (Shaw, 1954; Leavitt, 1951) by reducing errors in performance (Bavelas, 1950). Although hierarchical structures are not always efficient, many organizational leaders like the ability to control information flow, which they would lose in less centralized networks (Lopez, Mendes, & Sanjuan, 2002). Nevertheless, because of limited information processing abilities of managers, large scale organizations frequently need to establish decentralized information processing structures (Radner, 1993).

Despite the advantages of centralized networks, many situations, particularly those that involve uncertainty, complexity, or rapid change, require decentralized network structures for good performance. For example, decentralized schools are more capable in adopting changes, even though centralized schools are more capable in adopting practices (Cilliê, 1940). Decentralized communication structures outperform centralized structures in complex problem solving (Mulder, 1960) and other highly complex tasks (Blau, & Scott, 1962; Brown, & Miller, 2000). Because some nodes are more important than others in centralized networks, disconnection of an important node can severely decrease the efficiency of a centralized information processing network. In terms of network integrity, decentralized information processing network structures are more robust than centralized structures (Kwon, Oh, & Jeon, 2007). This becomes increasingly valuable as the reliability of communication channels or availability of particular nodes decreases. Decentralized networks are particularly helpful in dynamic environments (Kapucu, 2006).

For emergency response teams, decentralization increases the speed with which situational updates reach the people who most need the information. Decentralization provides information that can be used to make sensible resource allocations (Van Zandt, 1999), and it is particularly important for communication in fast-changing environments (Dessein, 2002). Horizontal communication can improve coordination, so decentralization can be the most suitable structure for organizations that must coordinate their activities quickly (Alonso, Dessein, & Matouschek, 2008). Hastily formed networks, which are established during emergencies, are highly complex, and they work best with decentralized network structures (Denning, & Hayes-Roth, 2006). As the information processing demands increase, hierarchies experience overloads, and decentralized structures become preferable (Scott, 1992). For coordination of long-term emergency responses, decentralized communication can be crucial (Gibbons, 2007b).

G. MILITARY NETWORKS AND RELIABILITY CONCERNS

The capabilities and relative value of the nodes involved in Network Centric Warfare influence the network structure and communication pattern that can best coordinate their joint efforts. Network-Centric-Operations, the emerging war theory of the Information Age, "involves developing communications and other linkages among all elements of the force to create a shared awareness of operations" (Curtin, 2004, p. 2). They speed up decision making time for military troops by providing shared situational awareness of the battlefield. Technological innovations make the military environment more complex than what many other organizations face, so the decision making structures in many situations should be decentralized (Janowitz, 1959).

In order to meet the challenging threats of the post Cold War environment, NATO needs to change its awkward military structure toward a smaller, robust, rapidly deployable response force, called the NATO Response Force (NRF). Moreover, military command and control network structure also has changed from hierarchical network structure to decentralized network structure in which both vertical and horizontal information flow enhances the network. Technological improvements also help networks to increase the information sharing capabilities of the nodes. Differences in technologies, cultures and so forth make multinational communication tasks more difficult (U.S. Department of Defense, 2007).

Dekker's (2005) taxonomy is based on two fundamental concepts. This first is value symmetry, which defines NCW architecture as value-symmetric, in which all nodes have the same importance, or non-value-symmetric, in which some nodes are more important than others. The second concept defines the homogeneity/heterogeneity among nodes; it distinguishes centralized (hierarchical communication), request-based (decentralized, selective communication), and swarming (all-channel communication) architectures. According to the network structures defined by Dekker (2005), orchestrated swarming, in which the leader node is chosen temporarily on the basis of suitable position, current combat situation, or other transient factors, performs better than any other network structures during a search and rescue operation.

Assessment of individual assets without attention to the configuration and coordination of those assets overlooks opportunities to increase collective capabilities. This can lead to poor decision making (Lenahan, Charles, Reed, Pacetti, & Nash, 2007). In real life environments where nodes and links are sensitive to overloads and dynamic failures happen, homogenous networks perform better than heterogeneous networks. Dynamical effects are the problems caused by an avalanche of breakdowns over the network (Boccaletti, Latora, Moreno, Chavez, & Hwang, 2006). This is because many distant connections between nodes in homogeneous networks allow information to pass quickly, which makes the nodes adapt easily to dynamical environments, while homogeneous distribution of messages also lessens overload on particular nodes. Strictly hierarchical organizations may lose important information or delay information flow processes due to nodes' transferability or to link failures during emergencies. Establishing shortcuts between top levels and bottom levels make hierarchical organizations more robust against failures (Helbing, Ammoser, & Kühnert, 2006).

Control-free command and control, in which missions are distributed to subordinates, performs better than other command and control models (Alberts, & Hayes, 1995).

Rather than being efficient, “being maximized by minimizing the number of costly links needed to support a defined burden” (Dodds, Watts, & Sabel, 2003, p. 1) is more important for an organization. Decentralized organizational structures are less susceptible to overload and connection failures, which are the two factors that determine overall organizational network robustness (Dodds, Watts, & Sabel, 2003).

Knowledge exchange is the key point to peacebuilding activities. Networking peacebuilding activities with conflict regions’ numerous entities can offer many advantages in preventing conflicts. Networks are established to extend the reach and influence of members and to gain access to sources of knowledge that could improve practice. By networking, participants can advance the work of their individual organization and also promote the wider field of the network. Collaboration in networks may expose organizations to new ideas and knowledge, enhances and deepen critical thinking and creativity, and help avoid competition and duplication of activities. The light structure of networks may allow peace builders to respond quickly to new situations and take new initiatives without going through a heavy bureaucratic process. However, differing organizational capabilities, language barriers, and funding issues are major handicaps to knowledge exchange (Verkoren, 2006).

H. RESEARCH QUESTIONS

This study focuses on the following research questions:

- What are the differences between centralized and decentralized networks due to different levels of reliability?
- Is there an optimum network design that has minimum cost and maximum effectiveness?
- What are the effects of centralization, reliability, and number of connections on the multinational military operating in Afghanistan?
- In eastern Afghanistan, can NATO PRTs networks be optimized according to reliability, centralization and number of ties?

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESEARCH DESIGN

Our objective was to experimentally determine the effects of network characteristics on efficiency and effectiveness of emergency assistance among Provincial Reconstruction Teams (PRTs) and similarly interdependent organizations. The experiment includes two patterns of network reduction (from all channel to centralized and from fully connected to decentralized) comprising 32 phases, five communication reliability levels, and two geographic dispersion patterns (equally distant and mapped onto PRT locations in Afghanistan), for a total of 320 (network by reliability by geography) cells. Results of 50 simulations were averaged to produce a single data point in each cell.

The design is implemented in a discrete event simulation model on the basis of time. The assumptions in our model, the functional relationships and parameters with numerical values, and the distributions remain the same for each observation in order to examine network effects under controlled conditions. To support practical applications, the model represents realistic scenarios and decision making processes. For example, the International Security Assistance Force (ISAF) in Afghanistan is experiencing resource problems. For that reason, our model cannot use huge resources in its logistic systems.

We begin with an all-channel (fully connected, and therefore decentralized) network, and then reduce the number of active ties, one by one, moving toward a centralized network. Then we return to the all-channel network and reduce the number of active ties, one by one, and keep a decentralized network. These processes result in two different streams of network design, one that remains fairly decentralized and one that becomes increasingly centralized as network density diminishes. The mean of ties ((Number of ties)/(Number of pairs)) and centralization are measured for each network structure.

Within each network structure, we vary the probability that attempted transmissions will be received. The range from 100% to 20% communication reliability represents decreased information flow that may follow from electronic counter measures, failure of apparatus, and human factors such as language problems in a multinational environment.

Finally, all network and reliability conditions are run (i) under an assumption of equal geographic distance among member nodes and (ii) the actual geographic locations of PRTs in eastern Afghanistan. The equal-distance assumption holds proximity constant to enable causal attributions of results to network characteristics. The Afghanistan case provides a field-based application of the model and enables comparison of the effects of uneven geographic dispersion.

Outcomes include number of PRT defeats, the average time before a terrorist attack is contained, number of supporting land and air forces that arrived late, and number of redundant messages. Redundant messages are the total of all kinds of messages that are received more than once by each PRT. If a message arrives at its destination, repetition of the exact same messages will be counted as redundant messages.

In the following paragraphs, the environment for our models, the network configurations, and the modeling procedures will be discussed.

A. THE ENVIRONMENT: RECONSTRUCTION TEAMS AND TERRORIST ATTACKS

Reconstruction teams are probable targets of terrorists who want to prevent delivery of social and economic aid to residents. As in the real world, attacks happen in our models at night and during the daytime throughout the year. We model a year as 365 sequential 24-hour days. The models run for a period of five years. Each five-year period is replicated 50 times under each condition, and the results are averaged. Fifty replications are adequate to predict the average response time with a 95% confidence interval of less than one minute

1. Frequency and Strength of Terrorist Attacks

Using the Worldwide Incident Tracking System (U.S. National Counterterrorism Center, 2008), we searched all terrorist incidents that happened in Afghanistan from April

1, 2003 until April 1, 2008. The total number of incidents was 2736. According to the Progress in Afghanistan report of NATO's Bucharest Summit (April 2-4, 2008, p. 7), security incidents in our exemplary province (east of Afghanistan) in 2007 made up 10% of total incidents. We applied this rate to the five year total: in the modeled region in five years, presumably 274 incidents happened. This equates to 1.05 incidents per seven days on average, so in our models, a terrorist attack occurs randomly about once per seven days.

In 2006, terrorist attacks were distributed as follows: armed attack 49%, bombing 27%, kidnapping 11%, arson 4%, assault 3%, suicide bombing 2%, hostage 1%, other 1% (U.S. National Counterterrorism Center, 2007). Table 1 translates these proportions of terrorist attacks into strength attributes with a normal distribution which has a mean of 100 and standard deviation of 40. This distribution allows an accurate proportion of attacks, such as suicide bombing, kidnapping, arson, bombing, and assault, to fall within the capability of one land support package. This support can include medics, explosive ordnance or demining unit teams but not air support. Similarly, an accurate proportion of attacks requires help from two or more land support teams, and likewise a proportionate need for air support.

Table 1. Strength attributes of terrorist forces in the models

Relative Strength of Terrorist Attack	Type of Attack	Probability to occur in the model (%)	Real Rate in 2006 (%)
0-60	Suicide bombing, kidnapping, arson	15.9	2+11+4
61-100	Bombing and assault	34.1	27+3
101-180	Armed attack	47.7	49
181- up	Heavy armed attack	2.3	

2. Strength of PRTs and Air Support for Response to Terrorist Attacks

We assumed all PRTs have response value of 60, and if they receive help from another PRT, the support's strength is 40. There is an air component which has response strength of 150. To successfully end a terrorist attack, the sum of response strength must equal or exceed the attack strength.

3. Geographic Distances among PRTs and Air Support Headquarters

There are six PRTs and an air support component in the models. We chose six PRTs as follows: Panjshir (U.S. operated), Nurestan (U.S. operated), Mihtarlam (U.S. operated), Jalalabad (U.S. operated), Asadabad (U.S. operated), Wardak (Turkey operated) and the ISAF air component located in Kabul. Terrorist attacks happen with equal probability for the PRTs. For the general models, distances between all reconstruction teams are equal and each reconstruction team's distance from air support is equal. For the Afghanistan case, distances among PRTs and headquarters are calculated using the country distance calculator from the website globefeed.com.

4. Responding to Terrorist Attacks

When attacked, a PRT sends messages to its contacts, informing them of the initial attack and updating them as events progress. Depending on the kind of attack, the PRT's active or inactive condition, and the distance to the attacked location (in the Afghanistan case), other PRTs may send land support and the headquarters may send air support.

5. Information Flows among PRTs and Air Support Headquarters

Three kinds of information flow between nodes in the simulation models:

1. Informative call: An attacked PRT produces this call to inform all other PRTs and the Air Support Headquarters. The call is created at the time of attack, and it automatically includes a request for help. Reliability of communication varies from 20% to 100%, represented in the models by adjusting the probability that each intended transmission will reach its

destination. By systematically varying communication reliability, we are able to test effects of network attributes under more or less favorable communication conditions.

2. Air Support call: This call is produced for just the Headquarters of Air Component, only in case of armed attacks. The request can be rejected by the headquarters, based on strength of the attack. This probabilistic component in the model reflects the tactical decision about the necessity of sending air support. An attacked PRT can renew the request after about ten minutes, and the probability of receiving air support increases as the attack continues.
3. Report call: This call informs Headquarters and other PRTs of the current situation, such as casualties or damage. We include report calls in our model because they are sent in the real world. Personnel are considering these reports, so the number of report calls that must be handled increases communication burden.

Each incoming call is transferred to immediately adjoining nodes, extending the potential message range (moderated by communication reliability) to two steps from the source of the message.

6. Decision Making and Delivery of Assistance

When a call for help is received, an information assessment and decision making process determines if a land support package will be released or not. A general military decision making process is composed of the following steps (U.S. Army Logistics Management College, 2003):

Step 1. Receipt of Mission

Step 2. Mission Analysis

Step 3. Course of Action (COA) Development

Step 4. Course of Action Analysis

Step 5. Course of Action Comparison

Step 6. Course of Action Approval

Step 7. Orders Production

This process includes determining the sort of attack, and comparing the distance between the attacked PRT and supporting PRT. A decision making process which requires 15 minutes (with a triangular distribution of 10, 15, 25 minutes) to release land support, includes preparation time. In the simulations, land support travels with an average speed of 40 mph to reflect estimated speed of armored vehicles in combat areas (West-Point Organization, 2002).

When a call for air support is received, an information assessment process and a decision making process take place in HQ in order to release close air support. The decision process includes determination of the need for air support, according to the heaviness of the attack. Following a decision to release air support, preparation requires 33 minutes, in accordance with statistics of turnaround times for fighter aircraft (Stillion, & Orletsky, 1999). In the simulation models, the travel time for air support equals six miles per minute, slightly below the flight speed of an A-10 aircraft (380 knots, or approximately 0.66 mach) during close air support (CAS) missions (Pirnie, Vick, Grissom, Mueller, & Orletsky, 2005)

7. Determining Outcomes

The information transfer and decision making processes affect response time, which strongly predicts damage and casualties in the real world. Each sort of information has different consequences for the success of overcoming a terrorist attack. An air support call causes a release of air support and an informative call is sent to receive land support. All messages are processed before support release, and each process causes a delay in reaction. According to the kind of attack, these supports' arrival times are calculated in the model.

Defeats of friendly forces preclude their assistance in subsequent attacks on neighboring PRTs. This increases the chance that terrorist attacks immediately following one PRT defeat will also be successful.

B. NETWORK STRUCTURES

The primary purpose of the simulations is to identify effects of PRT network characteristics on effectiveness and efficiency of response to calls for help given varying reliability of the communications. To systematically produce a range of centralized and decentralized networks, we implemented two progressions of network structures. Both progressions started from a fully connected network and deleted one tie at a time, but one deletion pattern moved toward a centralized network and the other remained decentralized. The mean of ties and degree of centralization were measured for each of the network structures, and all conditions ran at each stage of the network transformation.

1. Centralized Progression of Network Structures

To move toward centralization while reducing density, we chose one PRT that would retain all of its ties, and we incrementally removed the ties between all other PRTs (see Figure 4). In the general model, distances between PRTs are identical, so it doesn't matter which PRT we selected to be central. For the Afghanistan case, we randomly selected Wardak as the central PRT. It is relatively close to the HQ and acts as a bridge of communication.

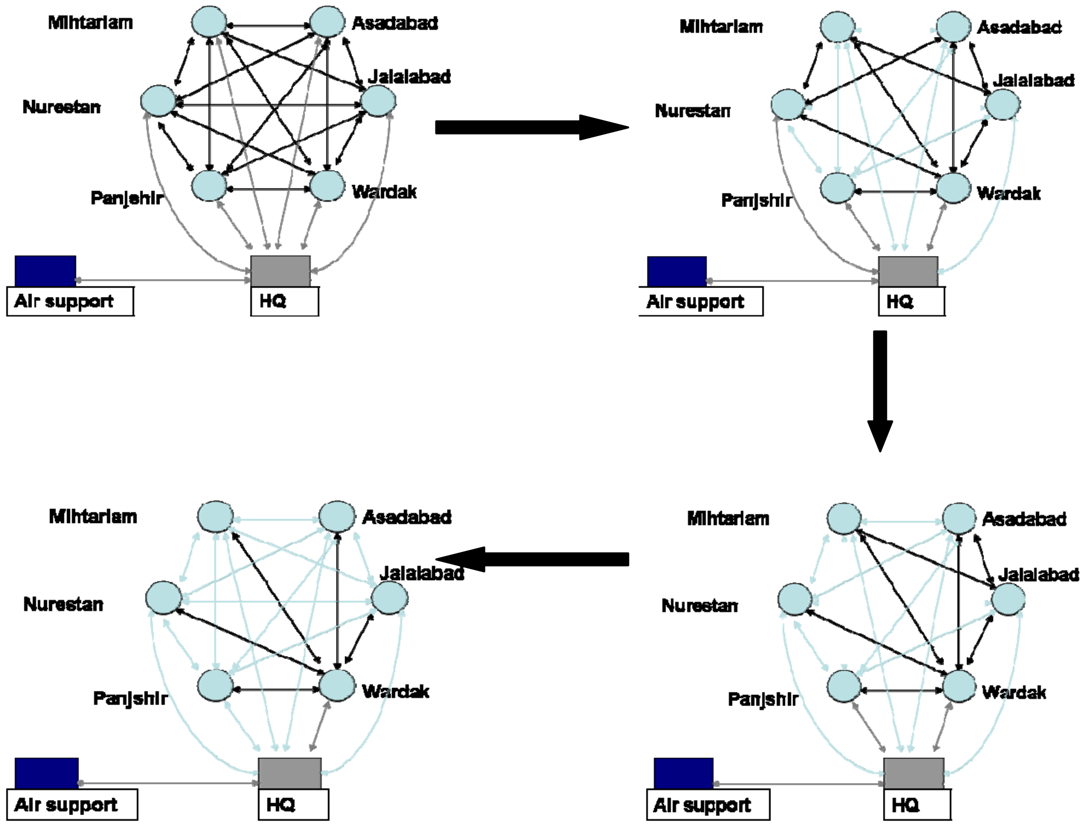


Figure 4. Centralized progression of network structures

2. Decentralized Progression of Network Structures

To remain decentralized structure while reducing density, we incrementally removed ties to the PRTs that had the highest (in-degree) ties in the network. At each step, we cut one tie to the PRT that had the most ties at that time, stopping when each PRT had only one tie to another PRT. We also retained a connection from one member of each dyad to the HQ of air support, so that information from all PRTs would reach the HQ (see Figure 5). Because distances between PRTs are identical in the general model, it doesn't matter which PRTs are paired. For the Afghanistan case, the pairs in our final decentralized structure—Jalalabad-Panjshir, Nurestan-Asadabad, and Wardak-Mihtarlam—are randomly formed.

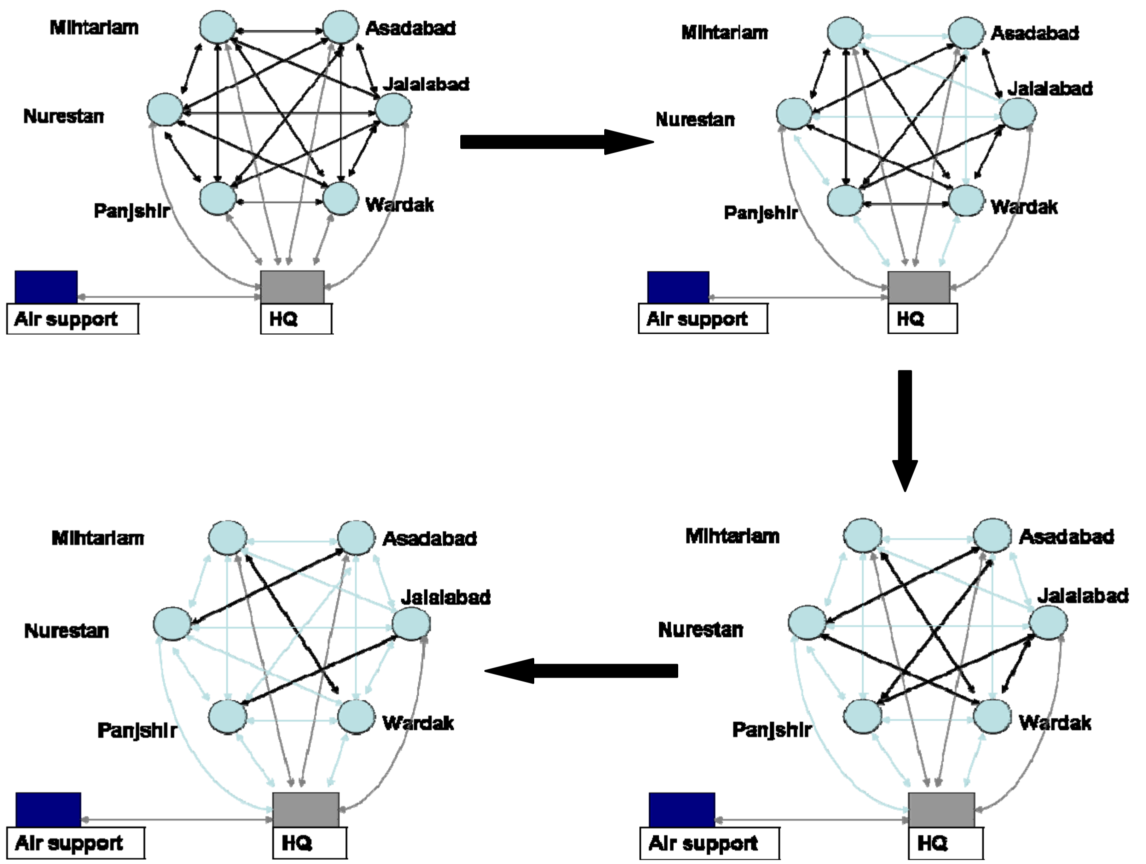


Figure 5. Decentralized progression of network structures

C. MODELING PROCEDURES

The simulation models were constructed using Arena (Kelton, Sadowski, & Sturrock, 2007). The procedures incorporate actors, the objects on which they operate, and the actions that they are allowed to take. Some of the actions are deterministic, while others occur probabilistically. We will first identify the actors and objects, and then outline the specific rules that guide actions and determine consequences. The simulation flowchart appears in Figure 6.

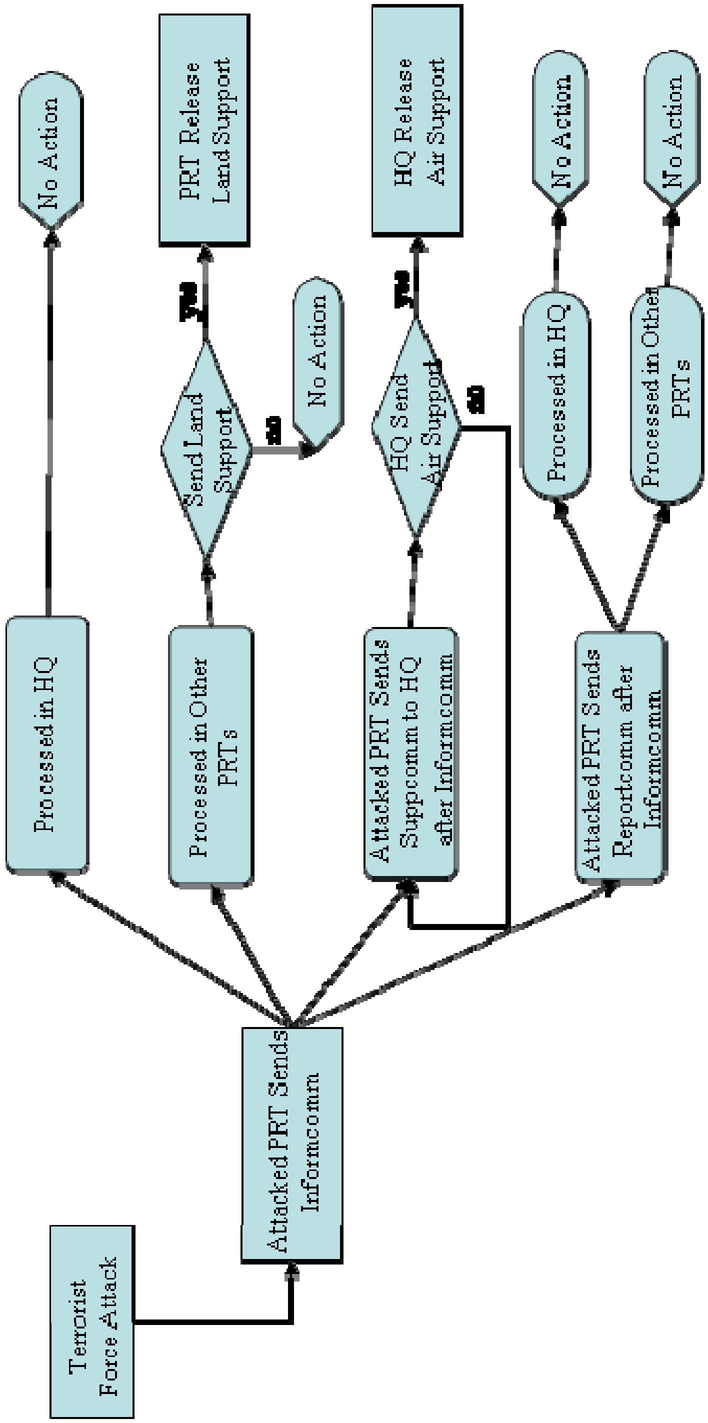


Figure 6. Simulation flowchart

1. Actors and Objects

The simulation models include three actors: PRTs (Provincial Reconstruction Teams), terrorists (Taliban forces attacking these NATO units), and headquarters (Air component of NATO located in Kabul). Actors produce or move the following objects:

- Informcomm: This is the first call that gives the initial information about the terrorist attack.
- Suppcomm: If the terrorist attack is an armed or (heavy armed) attack, this message is used for an air support call.
- Reportcomm: This message includes the information of current situation during the attack.
- Land force: This is the released force from a PRT to support an attacked PRT.
- Air support: The support force released by air component in Kabul to help the attacked PRT.
- Terrorist attack: The force released by a terrorist group against a PRT.

2. Rules Governing Response to Requests for Assistance

Informative calls are produced in the beginning of an attack as a one-time action. Thereafter, if the terrorist attack strength exceeds 100 air support calls are produced approximately every ten minutes, with actual time drawn from a normal distribution with a mean of ten minutes and standard deviation of two minutes. Report calls are produced approximately every five minutes during an attack, with actual time drawn from a normal distribution having a mean of five and standard deviation of one minute. All calls are distributed to partner PRTs and HQ at the same time.

PRTs that are not under attack transfer the information to their immediate contacts as soon as they have processed the information. If it is an air support call, it will be transferred to HQ only. But if it is informative call or report call, it will be delivered to all PRTs and HQ. The process is the same for all messages, not only for first ones. The HQ of the air component is never attacked and does not transfer any information except to inform the attacked PRT of air support rejections.

As mentioned earlier, informative calls require about 15 minutes of processing (with a triangular distribution of 10, 15, 25 minutes) as a first reaction to the attack on a neighboring PRT. The triangular distribution is a continuous distribution defined on the range $x \in [a, b]$ with a probability density function. Thereafter an incoming informative call to a PRT enters a decision making process for 15 minutes (with a triangular distribution of 10, 15, 25 minutes), which represents preparation time to respond or refuse assistance.

$$P(x) = \begin{cases} \dfrac{2\,(x-a)}{(b-a)\,(c-a)} & \text{for } a \le x \le c \\[2ex] \dfrac{2\,(b-x)}{(b-a)\,(b-c)} & \text{for } c < x \le b \end{cases}$$

Subsequent incoming calls (support and report calls) require about four minutes (normally distributed with the standard deviation of one minute) for information assessment and decision making. This shorter time assumes that the initial processing of the informative call has prepared the receiving PRTs for further transmissions. After these processes, all calls are transferred to adjoining nodes. Transferred messages are not forwarded beyond two steps from the original sender. The path length equaling 2 provides a capability of centralized networks to act as gateways in the model because it is not reasonable to preclude the central node from transferring the information.

In the general model, only the first PRT to complete its internal processing of an informative call about an unarmed attack sends assistance. If the attack is severe (greater than 100 attack strength), all PRTs who receive the informative call send help. In the Afghanistan case, decisions to send land forces depend on the distance between PRTs. Following receipt of an informative call requesting help, if the strength of attack is less than or equal to 100, the nearest PRT support force will be released. If the attack strength exceeds 100, the PRTs which are within 100 miles will respond. After release of PRT support forces, travel time to the attacked PRT is directly related to geographic distance. The travel time can be defined as a normal distribution with mean of (distance between

PRTs) 40 and with standard deviation of 10%. In the general case, the distance between PRTs is 100 miles, so the mean travel time is 2.5 hours for land support and 16.6667 minutes for air support.

Report calls will be filed in the PRTs after the transfer, which means disposed and removed from the system.

3. Battle Processes and Outcomes

An attack continues unless the strength attribute of PRT becomes greater than the strength attribute of terrorists. If the terrorist strength is less than or equal to the PRT strength, the first support arrival will finish the action in that PRT. We assume that this support is needed to bring medics, explosive ordnance/de-mining specialists, an intelligence team, etc. If no support or inadequate support reaches the PRT in five hours, the PRT is defeated or considered as unsuccessful. The five-hour cutoff follows from estimates that a 150 unit platoon will be defeated in four hours if the attackers have substantially higher capability than the defenders (Jaiswal, 1997). If one of the PRTs is defeated, it will be inactive for about a month, normally distributed with mean of 30 days and standard deviation of 10 days. If all six PRTs become inactive at the same time, no terrorist attack occurs because no PRTs are functioning.

When outgoing land support reaches the attacked PRT, the strength of that PRT increases by 40 units. If the strength of support force is still inadequate, the combat will go on and wait for further support. As soon as the strength of the PRT exceeds the strength of terrorists, the attack ends, and supporting forces return to their home PRTs. Forces that arrived after the attack is finished also return to their home sites. The returning forces require three times the travel interval before they will be available at their PRT.

An incoming call to HQ is processed in the information assessment section within about two minutes (normally distributed with standard deviation of 30 seconds) for air support calls and report calls. But the first call (which is an informative call) will be processed within 15 minute (with a triangular distribution of 10, 15, 25 minutes) as a first reaction to the attack. After information assessment in HQ, informative calls and report calls will be filed and removed from the system.

An incoming air support call to the HQ of the air component will initiate a decision making process in order to release air support after information assessment. But the request can be rejected by commanders in Kabul. For each request, the decision making interval will decrease while the number of requests increases. The time can be defined as a mean of (1/numberofrequest)*15 minutes which is exponentially distributed. We assumed that if the strength attribute of terrorists is greater than 140 the probability of a positive response to the first air support request is 75%, and 90% for the second request. We assumed that if the strength attribute of terrorists is less than 140 the probability of a positive response to a first air support request is 50%, and 75% for the second request.. In keeping with established estimates (RAND, 2005), we assumed that the third request will activate a positive response with 90% probability.

Following rejections of air support, the PRT resends the request about every ten minutes (standard deviation of two minutes) until the attack ends. When approved, air support requires a preparation time of about 33 minutes (Stillion, & Orletsky, 1999). Thereafter, the transportation time reflects distance and speed of flight.

When air support reaches the attacked PRT, the strength of that PRT increases by 150 units. As soon as the strength of PRT exceeds the strength of terrorists, the attack ends. Forces that arrive after the attack ends return to HQ at a speed of 40 miles per hour and require three times their travel time to be ready for a new release.

During all these processes, total average time of combat, time of combat for each specific PRT, number of land and air forces that arrived on time, number of land and air forces that arrived late, number of defeats for each PRT, number of messages used in the system, and number of redundant messages (measured as the sum of all duplicate messages received by PRTs and HQ, including informative, support, and report calls) are counted and recorded.

IV. ANALYSIS & RESULTS

In our model, the presence of ties and the reliability levels of ties change according to the scenarios. During the experiment, ties are taken out systematically for each run according to the rules. One of the rules causes the network to drift from fully connected toward centralized network, but the other one keeps it decentralized. We used the Unicet network analysis tool and saw that in our model, scenario 1 provides a stream of networks toward centralized network. Scenario 2 keeps the network decentralized (see Figure 7).

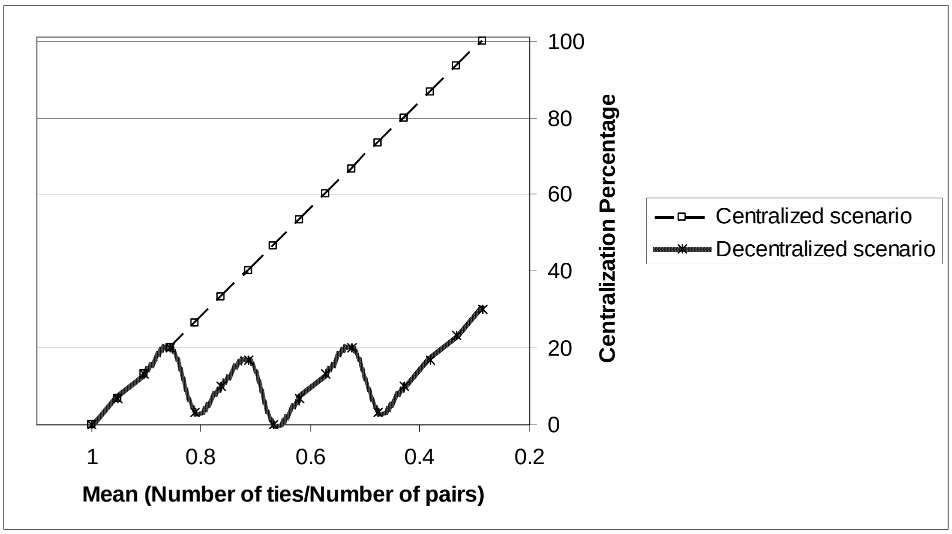


Figure 7. Centralization values of networks in both scenarios

The mean of ties of the network shows us the average number of ties for each node. It is calculated by (Number of ties)/(Number of pairs). In our runs we used the same number of pairs for all scenarios. For that reason, the number of ties shows the sequence of networks equally (with the mean of ties variable) Total combat time is the major output that shows the effectiveness of this network. More time means late reaction and causes more casualties. So, we looked for a network that provides less reaction time. In these two scenarios, we compared centralized and decentralized networks and got results for the variable named “number of active ties in network.” The fully connected network has 21 ties in both directions. But the 100% centralized network has 6 ties in scenario 1. In scenario 2, by keeping the decentralized structure, the minimum number of ties is 6 as well.

By obeying the rules we can obtain centralized and decentralized networks by various ways on the set of cutting tie actions. But what if the way we implemented these actions differs from other ways of similar actions? For example, in the scenario for the centralized network, we chose Wardak as central PRT (i.e., more important than the others). So, we started randomly to take the lines out from the fully connected shape network by keeping the ties which are connected to Wardak. What if the sequence of ties which are taken out is important to the results? In our model, the only difference between PRTs is the distance between nodes. By equalizing the distances between nodes we get a scenario in which the sequence of ties that are taken out is not important.

The outputs of the equal-distance version and the Afghanistan case model are similar. Both scenarios have the same significance level results. These results demonstrate that the sequence of ties that are taken out is not an important factor in our test.

A. RESULTS OF GENERAL MODEL

Total time of attack has two different characteristics in two different network types. As seen in Figure 8, the first model is more linear if the network is centralized. All trendlines are drawn in a second degree polynomial regression. In Figure 9, the reliability level of the connections causes significant changes in the lines.

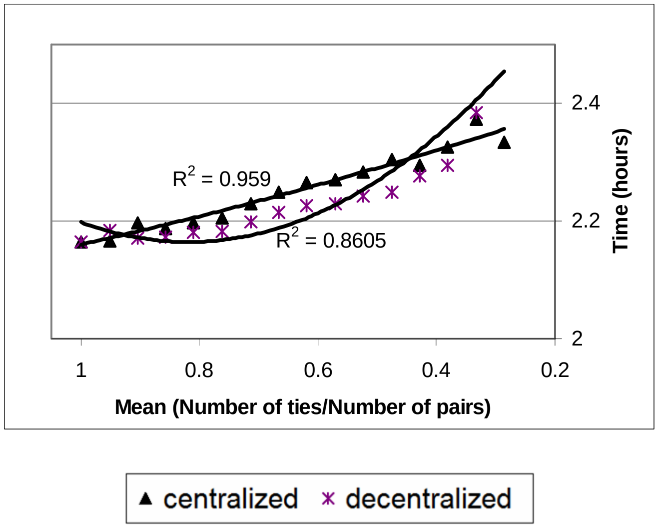


Figure 8. Total combat time (reliability %100)

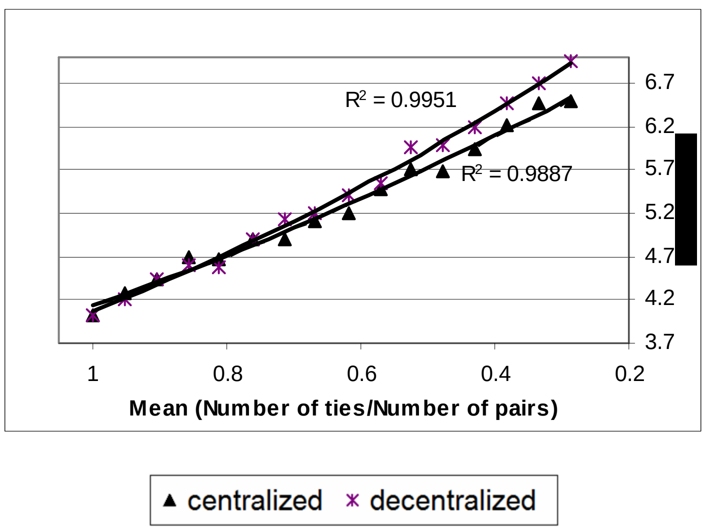


Figure 9. Total combat time (reliability %40)

In the Z score graph the y axis shows us the Z score values, while X axis is the mean (number of ties/number of pairs).

We chose four different outputs to show the graphs of cost and effectiveness. Total time of attack and number of defeats are the indicators of effectiveness. Redundant messages and land support which arrived late are the cost of our network. We only used land support because air support results have no significance according to the regression analysis. As seen in the following graphs, we used second- and third-degree polynomial regression on the outputs.

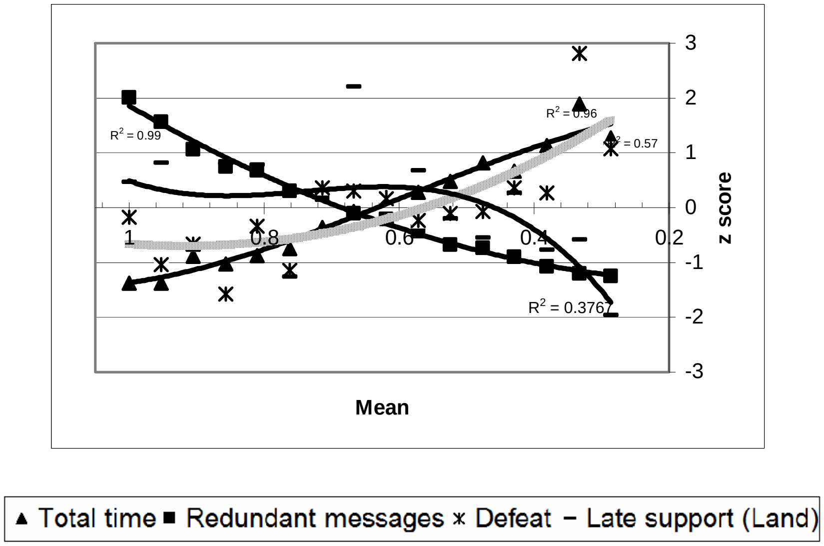


Figure 10. Z score graph (centralized model with 100% reliability)

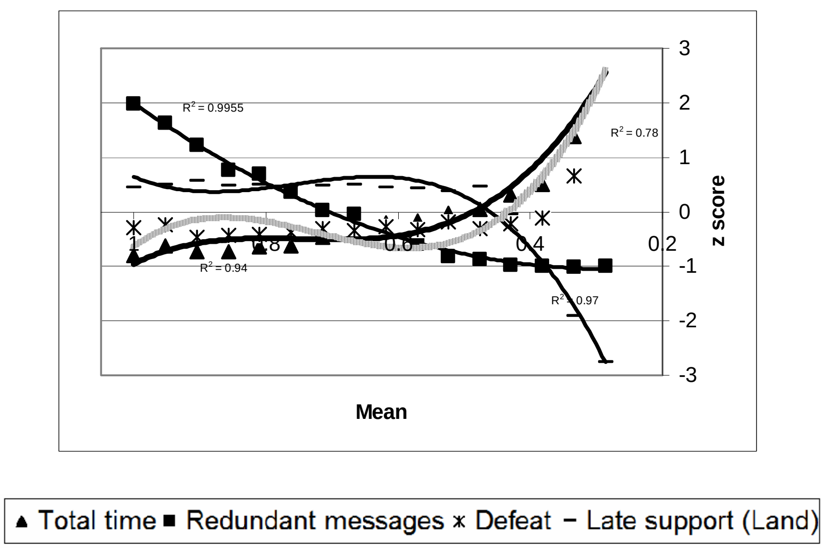
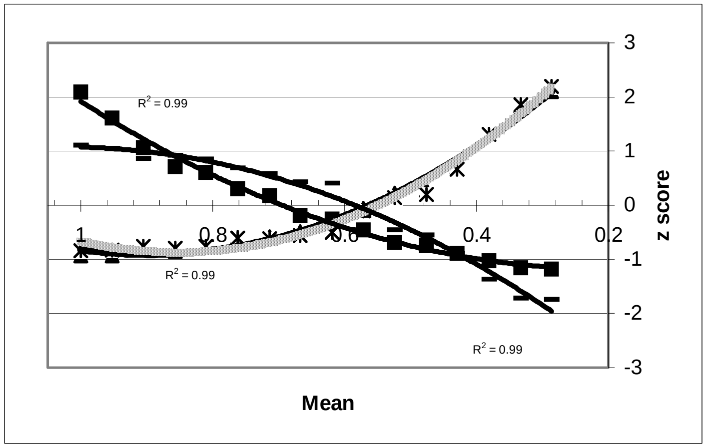
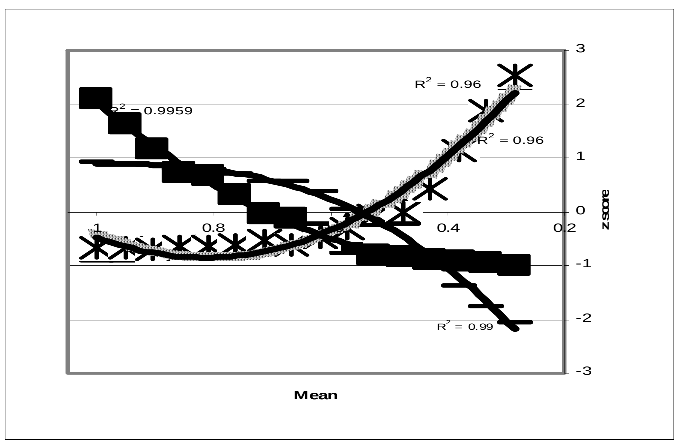


Figure 11. Z score graph (decentralized model with 100% reliability)



▲ Total time ■ Redundant messages ⁎ Defeat – Late support (Land)

Figure 12. Z score graph (centralized model with 80% reliability)



▲ Total time ■ Redundant messages ⁎ Defeat – Late support (Land)

Figure 13. Z score graph (decentralized model with 80% reliability)

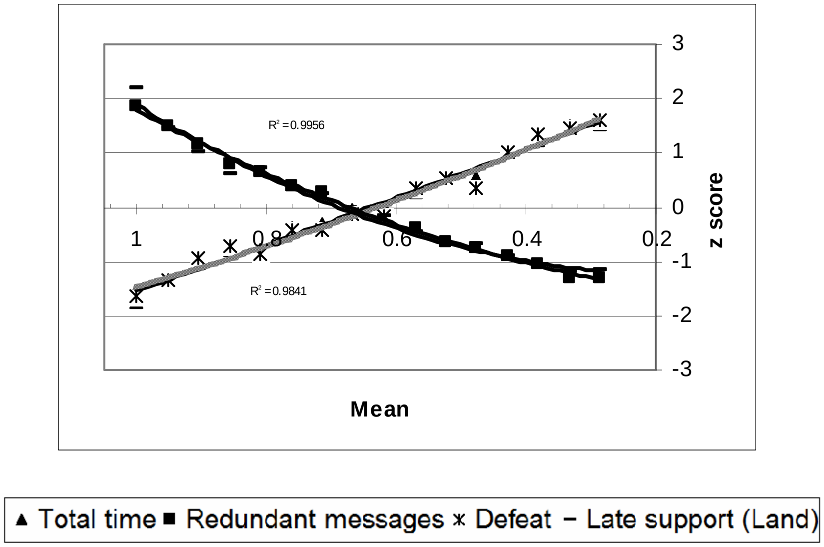


Figure 14. Z score graph (centralized model with 20% reliability)

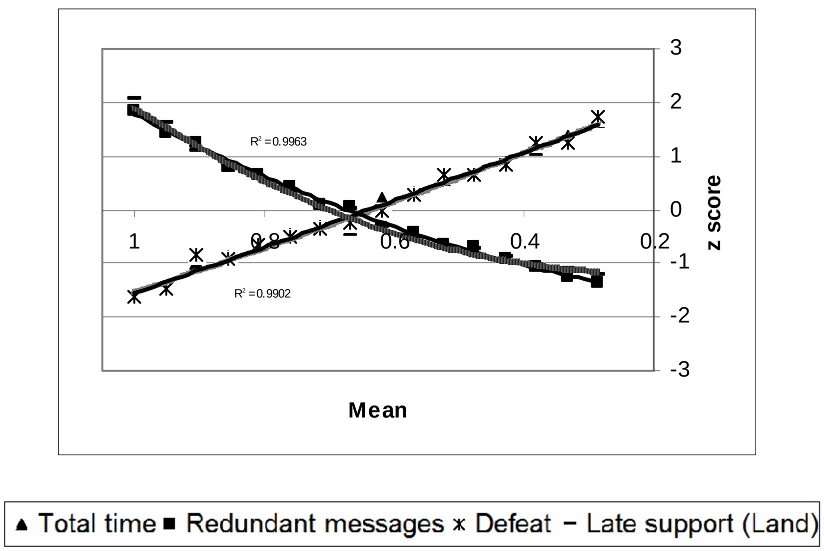


Figure 15. Z score graph (decentralized model with 20% reliability)

B. RESULTS OF AFGHANISTAN CASE MODEL

In the Afghanistan case, when we compared scenarios we saw that by decreasing the number of active ties, the total time of combat increases. However, decentralized networks are more reactive than centralized network (see Figure 16). In other words, centralized networks are less affected by the number of active connections. For decentralized networks the number of active ties is an important factor in our model.

If the rate of successful information transfer decreases, we saw that the regression curves become more linear and the slope of trend lines in the graphs increases (see Figure 17). This means that for less reliable networks number of active ties is more important, which is obvious. But these centralized networks' results are becoming closer to the decentralized networks' results which means that for less reliable centralized networks, the number of active ties is a more important factor.

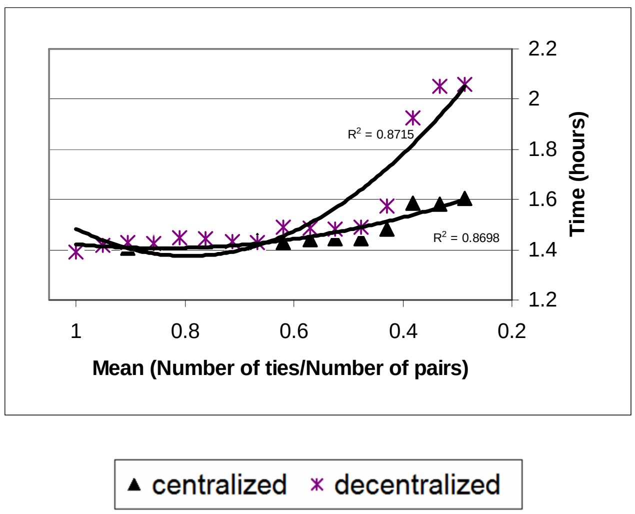


Figure 16. Total combat time (reliability 100%)

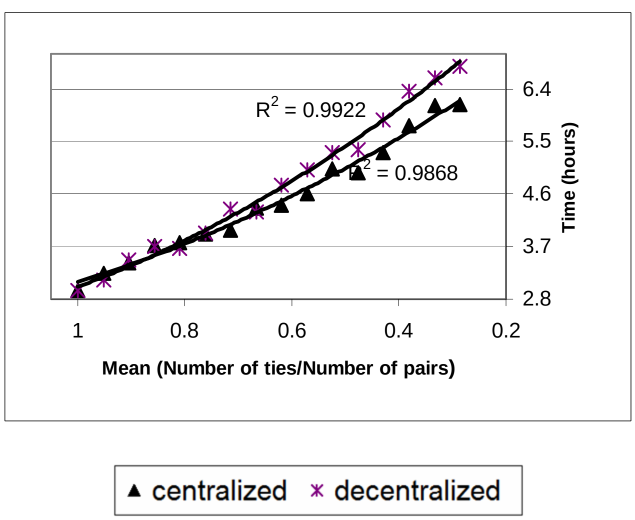


Figure 17. Total combat time (reliability 40%)

The other effectiveness unit in the model is the total number of defeats, which means no support has arrived within five hours. To compare defeat levels is easier if the number of active ties is very low. By keeping the network decentralized, we saw that if the number of active ties decreases, the number of defeats increases faster (see Figures 18 and 19). On the other hand, centralized networks are more resistant to the low number of active lines in terms of defeat numbers. But if the reliability level decreases, the difference between centralized and decentralized networks is less.

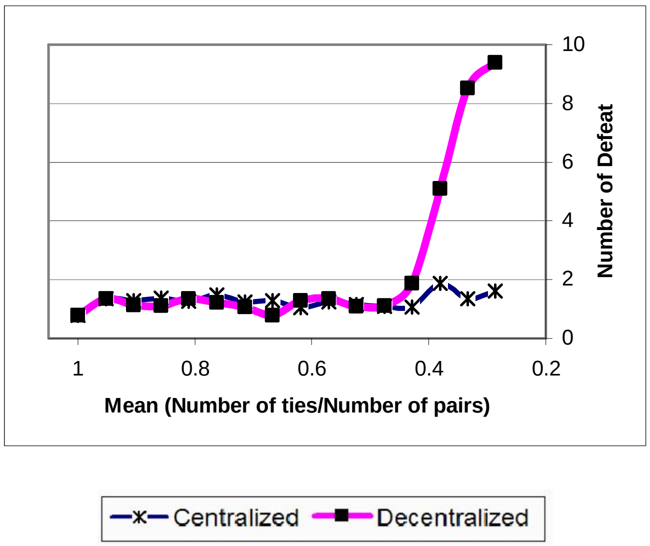


Figure 18. Total defeat (reliability 100%)

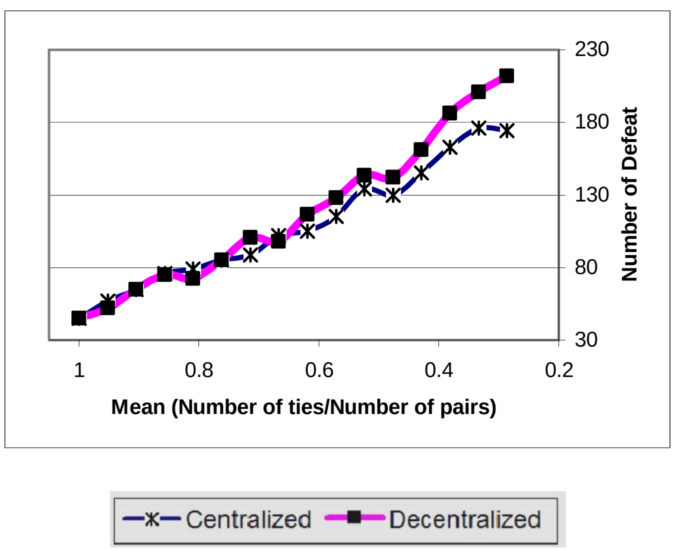


Figure 19. Total defeat (reliability 40%)

Table 2 gives the basic effectiveness indicator results of our network structures.

Table 2. Results of total time and defeat counter

		Centralized			Decentralized		
	Reliability level / # of active lines	100%	60%	20%	100%	60%	20%
Reaction Times (hr)	21	1.39	2.02	5.28	1.39	2.02	5.28
	20	1.41	2.11	5.58	1.42	2.05	5.45
	19	1.41	2.20	5.72	1.43	2.22	5.64
	18	1.43	2.34	5.86	1.43	2.30	5.77
	17	1.43	2.42	5.93	1.45	2.34	5.83
	16	1.43	2.58	5.98	1.44	2.53	6.04
	15	1.43	2.56	6.03	1.43	2.83	6.18
	14	1.44	2.88	6.30	1.43	2.83	6.27
	13	1.43	2.93	6.29	1.49	3.12	6.42
	12	1.44	3.05	6.39	1.48	3.44	6.60
	11	1.45	3.45	6.60	1.48	3.76	6.78
	10	1.45	3.47	6.59	1.49	3.79	6.83
	9	1.48	3.80	6.73	1.57	4.65	6.96
	8	1.59	4.43	6.98	1.92	5.51	7.11
	7	1.58	4.82	7.12	2.05	5.89	7.31
	6	1.60	4.90	7.12	2.06	6.25	7.36
Number of Defeats (times)	21	0.78	10.92	144.30	0.78	10.92	144.30
	20	1.34	14.58	153.24	1.34	12.64	149.90
	19	1.28	17.52	160.14	1.14	18.34	156.64
	18	1.38	22.36	165.04	1.12	21.28	163.64
	17	1.26	25.62	167.02	1.34	21.96	165.94
	16	1.48	32.36	173.08	1.22	29.20	174.66
	15	1.24	31.52	173.94	1.06	41.24	181.94
	14	1.28	41.76	188.50	0.78	40.14	183.54
	13	1.04	43.88	183.28	1.28	50.72	190.86
	12	1.24	51.06	192.00	1.36	63.52	198.50
	11	1.16	68.04	201.56	1.10	75.88	206.22
	10	1.08	68.86	198.50	1.12	78.44	204.80
	9	1.06	81.86	204.92	1.88	111.28	215.72
	8	1.88	105.74	215.12	5.10	143.96	223.80
	7	1.36	123.72	217.56	8.52	166.30	228.12
	6	1.62	124.40	220.32	9.40	184.56	236.60

The other important outputs about the simulation network design are redundant messages and late arriving support. Although late arriving support is an important output, we saw in the regression analysis that air support results are not significant according to the number of ties and centralization inputs. For that reason, we will focus on late land forces in order to determine resource problems. To understand the efficiency consideration of the model, we used the results of redundant messages and number of late arriving support (land) as costs. Total combat time and number of defeats could be recognized as the effectiveness scale of our simulation. But these results should be in the same units in order to compare them with each other. So, we calculated the z-scores of results and generated the graphs for five reliability levels (see Figures 20 to 25).

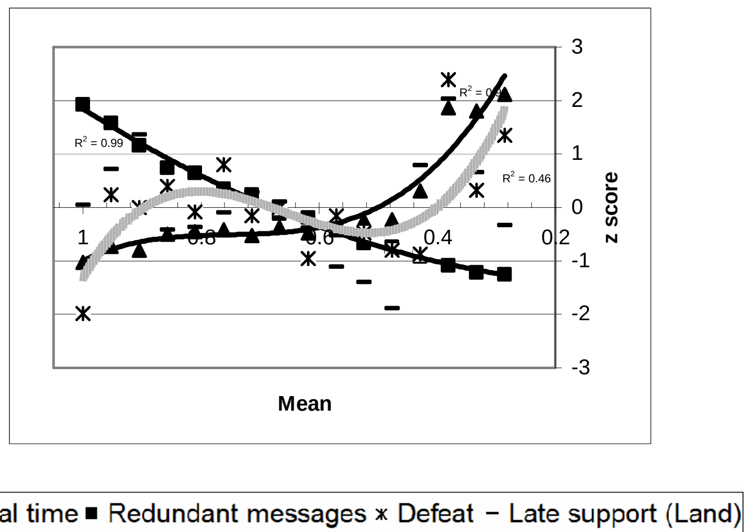


Figure 20. Z score graph (centralized model with 100% reliability)

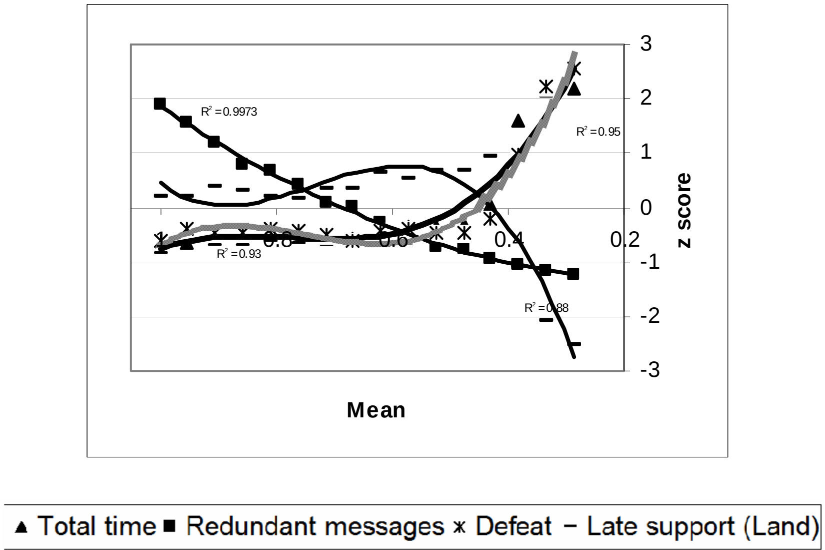


Figure 21. Z score graph (decentralized model with 100% reliability)

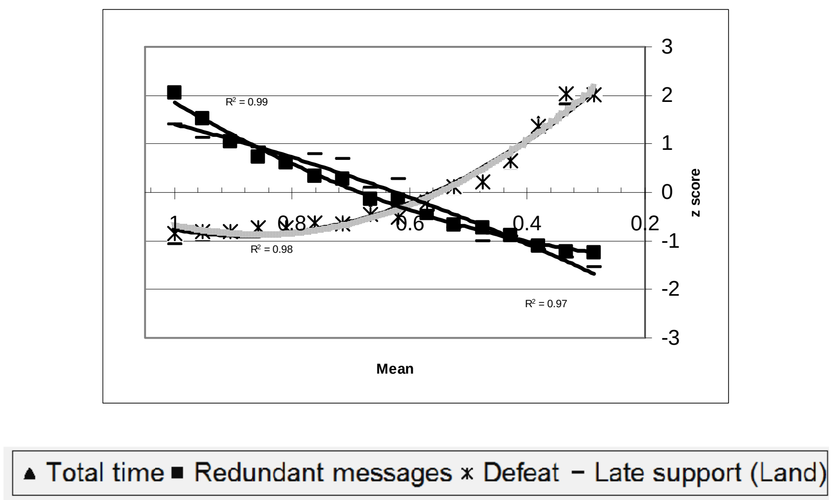


Figure 22. Z score graph (centralized model with 80% reliability)

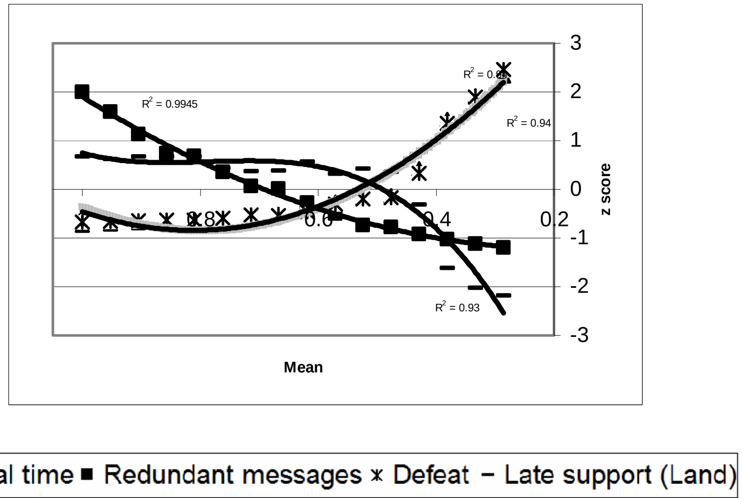


Figure 23. Z score graph (decentralized model with 80% reliability)

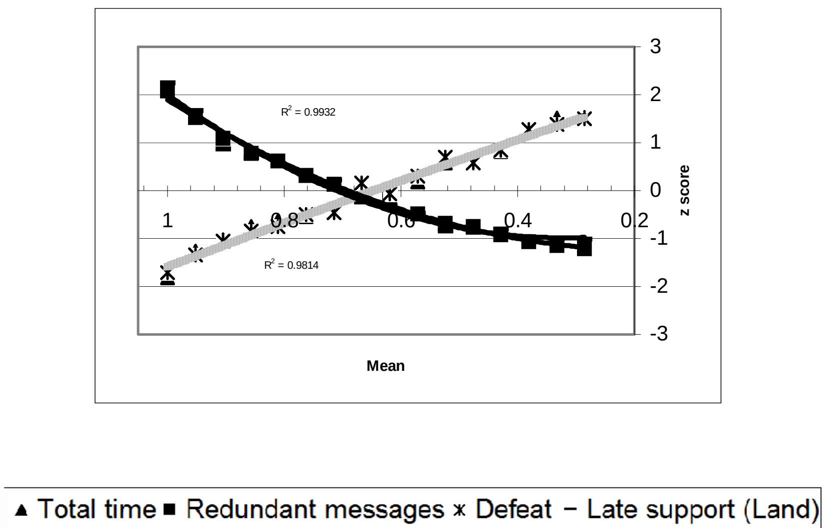


Figure 24. Z score graph (centralized model with 20% reliability)

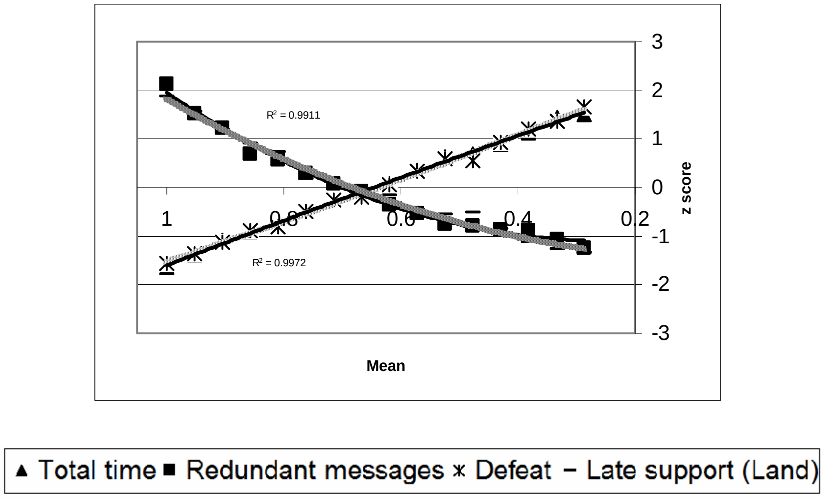


Figure 25. Z score graph (decentralized model with 20% reliability)

While reliability level decreases in both scenarios, total time and defeat results overlap, as do redundant messages and late support. In the model, redundant messages are the messages which are not used and do not affect combat. These messages are directly related to the number of ties between nodes. Late support is the number of support packages (both ground and air) which arrive to the attacked PRT after the fight ends. So, these two criteria symbolize the cost in our model. We can also view the report calls as cost. If the network structure is more efficient than others, the system will produce fewer report calls, fewer redundant messages and less late support. The used number of report calls strongly correlates with redundant messages (0.97426).

The effectiveness of networks can be measured by total combat time and number of defeats. These two outputs should have minimum values like redundant messages and late support. So, the most effective and efficient network structure is the intersection of these lines. Except for decentralized scenarios which have high reliability levels (see Figures 21 and 23) all graphs address a specific point as the optimum network structure. As seen in the graphs the optimum number of lines vary between 12 to 14. The optimum point slightly increases while the reliability level decreases. But the structure which is maintaining decentralization and high reliability has a significantly higher late support level as cost on the optimum point (See Figures 21 and 23). As explained in Chapter II, centralized structures have a more controllable structure in order to prevent poor resource allocation. As seen in the graphs, decentralized infrastructure causes more redundant resource allocation like late support due to lack of coordination. Our finding is that on less reliable occasions for decentralized structures, the system is more likely to prevent redundant usage of resources.

In our model, three criteria—number of active lines, reliability level, and centralization—are important to observe. We calculated the correlation between these variables and ouputs. As seen in Table 3, total combat time and defeat outputs are negatively correlated, while redundant messages and late support outputs are positively correlated with these variables.

According to the regression analysis (See Table 4) we see that reliability, density, and centralization have a negative relationship with the total response time and number of defeats. These effects are reduced as values increase, such that the importance of a unit increase in mean of ties at a low density has a greater impact on the outcomes than does a unit increase in mean of ties at a higher level of density.

Table 3. Descriptive Statistics and Correlation Matrix

		Mean	Std. Dev.	1	2	3	4	5	6	7	8	9	10
1	Total Time	3.989	1.828										
2	Defeat	82.622	75.613	0.984***									
3	Redundant Messages	1136.138	1466.372	-0.689***	-0.649***								
4	Late Support (Land)	299.439	334.045	-0.525***	-0.631***	0.446***							
5	Reliability	60.000	28.329	-0.875***	-0.874***	0.637***	0.617***						
6	Mean of Ties	0.643	0.220	-0.351***	-0.364***	0.536***	0.260***	0.000*					
7	Centralization	31.042	29.490	0.163**	0.170**	-0.269***	-0.092*	0.000*	-0.598***				
8	Centralization by Reliability	1862.494	2144.737	-0.244***	-0.244***	-0.051*	0.181**	0.410***	-0.493***	0.825***			
9	Centralization by Mean	16.092	12.407	0.058*	0.060*	-0.161**	-0.022*	0.000*	-0.345***	0.892***	0.736***		
10	Reliability by Mean	38.573	23.330	-0.859***	-0.858***	0.922***	0.645***	0.781***	0.565***	-0.338***	-0.021*	-0.195***	
11	Mean squared	0.461	0.286	-0.334***	-0.347***	0.547***	0.249***	0.000*	0.989***	-0.585***	-0.483***	-0.378***	0.559***

N = 320

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 4. Regression analysis of results

	Total Time		**Redundant Messages**		**Defeat**		**Late Support (Land)**	
	Model 1	Model 2	Model 1	Model 2	Model 1	Model 2	Model 1	Model 2
Reliability*	-0.875 (0.000)	-1.111 (0.000)	0.637 (0.000)	-0.894 (0.000)	-0.890 (0.000)	-1.194 (0.000)	0.856 (0.000)	0.264 (0.011)
Mean Ties*	-0.394 (0.000)	-1.507 (0.000)	0.584 (0.000)	-1.266 (0.000)	-0.389 (0.000)	-1.490 (0.000)	0.476 (0.000)	1.473 (0.000)
Centralization*	-0.073 (0.002)	-0.258 (0.004)	0.080 (0.039)	-0.095 (0.242)	-0.062 (0.031)	-0.232 (0.028)	0.163 (0.000)	0.313 (0.006)
Centralization by Reliability*		-0.006 (0.909)		0.174 (0.001)		0.014 (0.834)		0.286 (0.000)
Centralization by Mean*		0.170 (0.011)		0.023 (0.710)		0.141 (0.077)		-0.351 (0.000)
Reliability by Mean*		0.307 (0.000)		1.870 (0.000)		0.382 (0.000)		0.608 (0.000)
Mean squared*		0..895 (0.000)		0.790 (0.000)		0.848 (0.000)		-1.245 (0.000)
R-square	0.891	0.907	0.697	0.922	0.919	0.937	0.894	0.926
R-square change		0.016		0.225		0.019		0.033
F change	863.368	13.528	242.314	225.921	586.262	11.214	436.322	16.747
Decrease of Freedom (df1, df2)	(3, 316)	(4, 312)	(3, 316)	(4, 312)	(3, 156)	(4, 152)	(3, 156)	(4, 152)
Significance (p value)	> 0.001	> 0.001	> 0.001	> 0.001	> 0.001	> 0.001	> 0.001	> 0.001

* Numbers in the paranthesis are the p-values of related data

V. DISCUSSION & CONCLUSION

The imperfect nature of information transmission connections in a network, especially a military network during reconstruction activities, indicates that reliability issues should be considered for designing networks. Other important design variables include centralization and density of ties (shown as the network mean in our models).

The effectiveness in our models is significantly better given highly reliable connections. Total time of attack and total number of defeats are less. However, the number of redundant messages can be high. In both the general and the Afghanistan case model, the amount of support that arrives late is similar in the decentralized models. We found the optimized point of cost and effectiveness around network densities of 0.6 to 0.7 for all reliability levels.

A major difference between centralized and decentralized networks is that decentralized networks have poor resource allocation for highly reliable networks. Late support level is higher than the level in centralized networks. In our Afghanistan case, a network which has 12 to 14 connections among six PRTs has the most cost efficient results. The exception is the resource allocation of decentralized networks. At the point where the balance between successful response and redundant messages is optimized, the amount of land support that arrives too late to be helpful is greater in decentralized networks than in centralized networks. It is also greater than at other densities that are less optimal for successful response according to our other indicators.

We found that the influence of number of ties is greater in decentralized networks. In less reliable networks the reactions of decentralized and centralized networks are similar in terms of combat time and defeat. Fully connected networks have the least times of response and defeat numbers. The worst network design in our models was a decentralized network with density below 0.4. If we must keep the number of lines less than eight in our Afghanistan case, centralized design has significantly better results.

According to the previous findings, the optimum level of connections in our Afghanistan case is 12-14 ties. Centralized networks will provide more control and provide a better way of resource allocation. Furthermore, reliability of ties should be maintained as much as possible. For less reliable networks, centralized designs provide slightly better results than decentralized designs. The network shown in Figure 26 is an example of a high-performing network design for our Afghanistan case. This network is somewhat centralized, as all members maintain ties to Wardak while limiting their lateral ties.

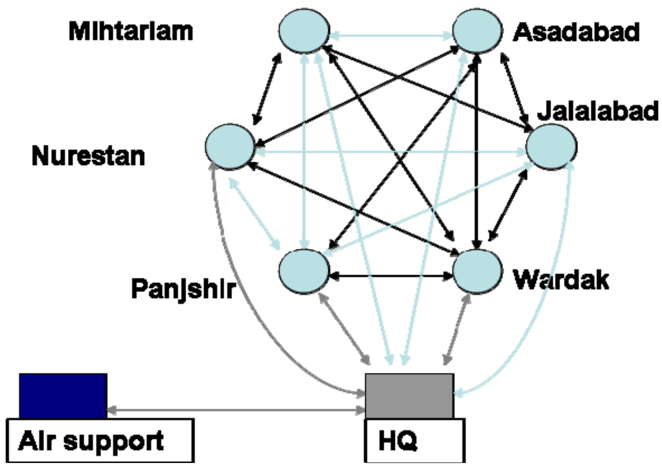


Figure 26. An example of optimum centralized network

In our general model design, all results are slightly different from our special case. The general and Afghanistan models produce similar results, but the outcomes of total time and late land support have changed depending on the distance arrangements. Despite the fact that the effect of geographic distances is different in both models, the results strongly correlate (r = 0.9995). So, the findings in our specific case of Afghanistan are also adaptable for similar kinds of network designs.

VI. POTENTIAL FUTURE PROGRESS ON RESEARCH

The primary limitation for our models was the scale of the network. We used only six nodes, but the models could be expanded, for instance, to include all of Afghanistan. Another recommended addition to the models can be the injection of multinational obstacles and caveat issues for NATO into the network model. In the scope of Forcenet studies, future research will benefit from explicit experimentation with network designs. Our results may serve as foundations for this research, while providing immediate assistance for decision makers who must design emergency response information networks in theater.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, D. S., & Hayes, R. E. (1995). *Command arrangements for peace operations*. Washington, DC: National Defense University Press.

Alonso, R., Dessein, W., & Matouschek, N. (2008). When does coordination require centralization? *The American Economic Review*, 98(1): 145-179.

Arrow, K. J. (1974). *The limits of organization.* New York: W. W. Norton.

Barabasi, A. L., & Albert, R. (1999). Emergence of scaling in random networks. *Science, 286*, 509–512.

Bavelas, A. (1950). Communication patterns in task-oriented groups. *The Journal of the Acoustical Society of America,* 22(6), 725-730.

Blau, P. M., & Scott, W. R. (1962). Formal organizations. San Francisco: Chandler.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D. U. (2006). Complex networks: Structure and dynamics. *Physics Reports*, 424(4-5): 175-308.

Bolton, P., & Farrell, J. (1990). Decentralization, duplication, and delay. *Journal of Political Economy*, 98(4): 803–826.

Bolton, P., & Dewatripont, M. (1994). The firm as a communication network. *Quarterly Journal of Economics*, 109, 4, 809-839.

Brown, T. M., & Miller, C. E. (2000). Communication networks in task-performing groups: Effect of task complexity, time pressure, and interpersonal dominance. *Small Group Research*, 31(2), 131-157.

Cilliê, F. (1940). *Centralization or decentralization.* New York: Teachers College, Columbia University.

Curtin, N. P. (2004). Military operations: recent campaigns benefited from improved communications and technology, but barriers to continued progress remain. *GAO Reports, 04-547,* Washington, DC.

Dekker, A.H. (2005, November). *A taxonomy of network centric warfare architectures.* Paper presented at Systems Engineering/Test and Evaluation Conference, Brisbane, Australia.

Denning, P. J., & Hayes-Roth, R. (2006). Decision making in very large networks. *Communications of the ACM,* 49(11), 19-23.

Dessein, W. (2002). Authority and communication in organizations. *Review of Economic Studies,* 69(4), 811-838.

Dodds, P. S., Watts, D. J., & Sabel, C. F. (2003). Information exchange and the robustness of organizational networks. *Proceedings of the National Academy of Sciences of the United States of America*, 100(21): 12516-12521.

Gallis, P. (2008). NATO in Afghanistan: a test of the transatlantic alliance. *CRS Report for Congress*. Washington, DC: Congressional Research Service.

Gibbons, D. E. (2007a). Interorganizational network structures and diffusion of information through a health system. *American Journal of Public Health, 97,* 1684-1692.

Gibbons, D. E. (2007b). Maximizing the impact of disaster response by nonprofit organizations and volunteers. In D. E. Gibbons (Ed.) *Communicable Crises: Prevention, Management and Resolution in the Global Arena.* Charlotte, NC: Information Age Publishing, 203-240.

Guetzkow, H. & Simon, H. A. (1955). The impact of certain communication nets upon organization and performance in task-oriented groups. *Management Science*, 1(3), 233-250.

Hart, O., & Moore, J. (2005). On the design of hierarchies: coordination versus specialization. *Journal of Political Economy*, 11 3(4): 675–702.

Helbing, D., Ammoser, H., & Kühnert, C. (2006). Information flows in hierarchical networks and the capability of organizations to successfully respond to failures, crises, and disasters. *Physica A: Statistical Mechanics and its Applications,* 363(1), 141-150.

ISAF History (2008, February). Retrieved April 20, 2008, from http://www.nato.int/isaf/topics/history/index.html.

Jaiswal, N. K. (1997). Military operations research: quantitative decision making. *International Series in Operations Research & Management Science,* Springer.

Janowitz, M. (1959). Changing patterns of organizational authority. *Administrative Science Quarterly*, 3(4), 473-493.

Kapucu, N. (2006). Interagency communication networks during emergencies: Boundary spanners in multiagency coordination. *American Review of Public Administration, 36*(2), 207-225.

Kelton, W. D., Sadowski, R.P., & Sturrock, D. T. (2007). *Simulation with Arena (4th ed.).* New York: McGraw-Hill.

Kwon, D., Oh, W., & Jeon, S. (2007). Broken ties: the impact of organizational restructuring on the stability of information-processing networks. *Journal of Management Information Systems*, 24(1), 201-231.

Leavitt, H. J. (1951). Some effects of certain communication patterns on group performance. *Journal of Abnormal and Social Psychology*, 46, 38-50.

Lenahan J., Charles P., Reed R., Pacetti D., & Nash M. (2007, June). *Mapping network centric operational architectures to C2 and software architectures.* Paper presented in 12th ICCRTS, Newport, Rhode Island.

Li, H. (1999). Hierarchies and information-processing organizations. *Review of Economic Design*, *4*(2), 101.

Lopez, L., Mendes, J. F. F., & Sanjuan, M. A. F. (2002). Hierarchical social networks and information flow. *Physica A: Statistical Mechanics and its Applications*, 316(1-4): 695-708.

Mason, W.A., Jones, A., & Goldstone, R.L. (2006). *Propagation of innovations in networked groups.* Unpublished manuscript, Indiana University —Bloomington.

McEnerney, J. X. (2001). Network centric logistics. *Strategy Research Project.* Pennsylvania: U.S. Army War College.

Mulder, M. (1960).Communication structure, decision structure and group performance. S*ociometry, American Sociological Association*, 23(1), 1-14.

NATO in Afghanistan Factsheet (2007, July). Retrieved April 18, 2008, from http://www.nato.int/issues/afghanistan/040628-factsheet.htm.

NATO. (2008). Retrieved May 5, 2008, from http://www.nato.int/isaf/docu/epub/maps/graphics/afghanistan_prt3.pdf.

NATO. (2008). *Progress in Afghanistan: Bucharest summit 2-4 April 2008*. Brussels: NATO Public Diplomacy Division.

Noetzel, T., House, C., & Scheipers, S. (2007). Coalition warfare in Afghanistan: burden-sharing or disunity? *Chatham House, Asia and International Security Programmes, Briefing Paper*, London.

Operation Enduring Freedom – Afghanistan. (2008). Retrieved April 18, 2008, from http://www.globalsecurity.org/military/ops/enduring-freedom.htm.

Perito, R., and Miller, L. (2004, March). Establishing the rule of law in Afghanistan. *United States Institute of Peace, Special Report 117* Washington, DC.

Perito, R. M. (2005). The U.S. experience with provincial reconstruction teams in Afghanistan: lessons identified. *United States Institute of Peace, Special Report, 152*, Washington, DC.

Pirnie, B. R., Vick, A., Grissom, A., Mueller, K. P., & Orletsky, D. T. (2005). *Beyond close air support: forging a new air-ground partnership*. Santa Monica: RAND Corporation.

Radner, R. (1993). The organization of decentralized information processing. *Econometrica,* 61, 1109-1146.

Scott, W. R. (1992). *Organizations: rational, natural, and open systems (3rd Edition).* New Jersey: Prentice Hall.

Shaw, M. E. (1954). Some effects of problem complexity upon problem solution efficiency in different communication nets. *Journal of Abnormal and Social Psychology,* 48, 211-217.

Stillion, J., & Orletsky, D. T. (1999). *Airbase vulnerability to conventional cruise-missile and ballistic-missile-attacks: technology, scenarios, and U.S. air force responses.* Santa Monica: RAND Corporation.

The War in Afghanistan, Operation Enduring Freedom: 2001-Present. (2007). Retrieved April 18, 2008, from http://www.historyguy.com/war_in_afghanistan.html.

U.S. Army Logistics Management College. (2003). Theater logistics handbook. Retrieved May 16, 2008, from http://www.almc.army.mil/LEDD/8a-f17/Adobe/V6-I-03%20--%20Staff%20Planning.pdf.

U.S. Department of Defense. (2006, April). Provincial reconstruction teams in Afghanistan - an interagency assessment. *Interviews of U.S. officials, 2006-2007*, Washington, DC.

U.S. Department of Defense (2003). *Network centric warfare: creating a decisive warfighting advantage.* Washington, DC.

U.S. Department of Defense. (2007, August). The evolution of NATO network-enabled capabilities: immediate reaction task force (land). Transformation *Case Study Series, Network Centric Operations Case Study, Abridged Report Version 1.0.* Retrieved May 6, 2008, from http://www.oft.osd.mil/library/library_files/document_407_IRTF(L)%20HBR.doc.

U.S. National Counterterrorism Center. (2008). *The worldwide incidents tracking system*. Retrieved May 16, 2008, from http://wits.nctc.gov.

U.S. National Counterterrorism Center. (2007). *Report on Terrorist Incidents – 2006*. Washington, DC.

U.S. Joint Forces Command Joint Warfighting Center (2007). Provincial reconstruction teams. *Pre-doctrinal Research White Paper, 07-01.*

Van Zandt, T. (1999). *Decentralized information processing in the theory of organizations.* In Sertel, M., editor, Contemporary Economic Development Reviewed, Volume 4: The Enterprise and its Environment. Macmillan, London.

Verkoren, W. (2006). Knowledge networking: Implications for peacebuilding activities. *International Journal of Peace Studies, 11*(2), 27-62.

West-Point Organization. (2002). *US Army Stryker interim armored vehicle: issues & questions.* Retrieved May 18, 2008, from http://www.west-point.org/publications/Stryker.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Robert N. Beck
   Dean, Graduate School of Business and Public Policy
   Naval Postgraduate School
   Monterey, California

4. Deborah E. Gibbons
   Graduate School of Business and Public Policy
   Naval Postgraduate School
   Monterey, California

5. James E. Suchan
   Graduate School of Business and Public Policy
   Naval Postgraduate School
   Monterey, California

6. Ali Bas
   9ncu Ana Jet Us 192nci Filo K.ligi
   Balikesir, Turkey

7. Volkan Karaca
   Hava Kuvvetleri K.ligi
   Ankara, Turkey

8. Hava Harp Okulu
   Hava Harp Okulu Kutuphanesi
   Yesilyurt, Istanbul, Turkey

9. Deniz Harp Okulu
   Deniz Harp Okulu Kutuphanesi
   Tuzla, Istanbul, Turkey

10. Kara Harp Okulu
    Kara Harp Okulu Kutuphanesi
    Bakanliklar, Ankara, Turkey